Patch Release Note

Patch 86251-08
For Rapier Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86251-08 for Software Release 2.5.1 on existing models of Rapier L3 managed switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86251-08.

Base Software Release File	86s-251.rez
Patch Release Date	9-Dec-2003
Compressed Patch File Name	86251-08.paz
Compressed Patch File Size	545820 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.5.1 for Rapier Switches (Document Number C613-10354-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in 86251-08

Patch 86251-08 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 03179 Module: IPG Level: 3

The device responded when it received a directed broadcast ICMP echo request that was in its supernet, but not its subnet. This issue has been resolved.

PCR: 03359 Module: CORE Level: 3

An incorrect object ID (OID) was being returned for Fan/PSU in SNMP v1 trap messages.This issue has been resolved.

PCR: 03527 Module: BGP Level: 4

Session-only counters have been added to the MIB entry for BGP peers.

PCR: 03622 Module: ENCO Level: 2

Interoperating with other vendors implementations of ISAKMP was occasionally causing errors following key exchanges. This relates to differing implementations of the RFC regarding the retention of leading zeros. This issue has been resolved by modifying the software to retain leading zeros. An additional command provides compatibility with routers that still use previous software versions. The command details are:

```
SET ENCO DHPADDING={ON|OFF}
```

This command controls the padding process for Diffie Hellman generated values. This may be required when interoperability is required with other vendor's equipment that uses the Diffie Hellman algorithm.

The DHPADDING parameter specifies whether the Diffie Hellman generated values should be padded or not. If ON is specified, then leading zeros will be inserted into the generated values. If OFF is specified, then the generated values will not be padded. The default is ON.

For example, to turn off the Diffie Hellman padding, use the command:

```
SET ENCO DHPADDING=OFF
```

Also, the output of the SHOW ENCO command now contains a new line showing the setting for DHPADDING.

PCR: 03684 Module: CORE Level: 4

A *fanAndPsRedundantFanTrap* message was sent from a Rapier when the RPS (Redundant Power Supply) was turned on or off, even though Rapiers do not monitor the redundant fan status. This issue has been resolved.

PCR: 03726 Module: TTY, USER Level: 3

The time recorded when a user logged in was overwritten when the same user logged in a second time while the original connection was still active. This meant the SHOW USER command displayed the same time for both connections. This issue has been resolved.

PCR: 03746 Module: BGP Level: 2

Occasionally a fatal error occurred if BGP debug was disabled. Also, BGP debug messages were sometimes still displayed after BGP debug was disabled. These issues have been resolved.

PCR: 03781 Module: STP Level: 2

A buffer leak occurred when rapid STP was specified with the SET STP MODE=RAPID command, but STP had not been enabled with the ENABLE STP command. This issue has been resolved.

PCR: 03856 Module: FIRE, UTILITY Level: 2

When a file was copied, only blocks of 1024 bytes were copied successfully. The remainder was discarded. This had two possible consequences. Either a truncated file was created on the destination media, or the device restarted with a fatal error. This issue has been resolved so that files copy correctly.

PCR: 03858 Module: IP

This PCR implements RFC 1256 "*ICMP Router Discovery Messages*". This enhancement allows the device to advertise its interface IP addresses to local hosts. For details, see "*ICMP Router Discovery Advertisements*" on page 47.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03873 Module: IPG Level: 4

The STATIC and INTERFACE options have been removed from the PROTOCOL parameter in the ADD IP ROUTE FILTER and SET IP ROUTE FILTER commands. These parameters were redundant because received static and interface routes are always added to the route table.

PCR: 03893 Module: FW Level: 3

Reverse enhanced NAT was not working for ICMP packets. This issue has been resolved.

PCR: 03926 Module: PIM Level: 2

Repeated *Assert* messages were sent after the prune limit expired. This issue has been resolved. The default dense mode prune hold time has been changed from 60 seconds to 210 seconds.

PCR: 03935 Module: ISAKMP Level: 3

ISAKMP debug messages now correctly output IPv6 addresses when using IPv6, and IPv4 addresses when using IPv4.

PCR: 03937 Module: IPSEC Level: 2

The IP version of packets was not being checked, so an IPv4 packet could match an IPv6 IPSec policy. This issue has been resolved.

PCR: 03953 Module: SW56 Level: 3

On AT-8800 series switches, strict QoS scheduling is now enforced for ports where egress rate limiting is applied. On Rapier *i* series switches, the same QoS setup is now applied to all of the appropriate ports when setting up egress rate limiting.

PCR: 03958 Module: FIREWALL Level: 2

The ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands no longer accept the GBLREMOTEIP parameter with standard NAT, or enhanced NAT for a private interface.

PCR: 03961 Module: PIM, PIM6 Level: 2

The PIM-DM prune expiry time was not reset when a *State Refresh* message was received. This issue has been resolved.

PCR: 03965 Module: IPSEC Level: 3

IPv6 used the same SA soft expiry timer at both ends of a link, which used memory unnecessarily. This issue has been resolved.

PCR: 03967 Module: IPG Level: 2

RIP did not send the correct next hop address if the route originated from a different subnet to that of the egress interface. This issue has been resolved.

PCR: 03970 Module: IPV6 Level: 3

If an IPv6 filter that blocked traffic on a VLAN interface was removed, the traffic was still blocked. This issue has been resolved.

PCR: 03973 Module: IPG Level: 3

When equal cost multipath routes were used, the IP option field for trace route was not applied correctly. This issue has been resolved.

PCR: 03978 Module: OSPF Level: 3

Occasionally an error occurred with OSPF's route table calculation, so all routes in the network were not discovered. The error only happened with a network topology that involved connections between routers via both a Point to Point link and a transit network link. This issue has been resolved. A new command has been added that forces a route table recalculation by rerunning the Shortest Path First calculation. The command is:

```
RESET OSPF SPF [DEBUG]
```

If DEBUG is specified, debugging information for the route table calculation is output to the port from which the command was executed. SPF debugging can be turned on for every route table calculation using the ENABLE OSPF DEBUG=SPF command, but this will be overridden if DEBUG is specified with the RESET OSPF SPF command.

PCR: 03982 Module: FIREWALL Level: 3

The SMTP proxy did not correctly filter sessions where messages were fragmented. This had the potential to prevent the detection of third-party relay attacks. This issue has been resolved.

PCR: 03985 Module: SWI Level: 2

Sometimes on Rapier series switches, a severe multicast or broadcast storm depleted packet buffers, so the switch received packets intermittently. This issue has been resolved.

PCR: 31000 Module: IGP Level: 3

In the output of the SHOW IP IGMP COUNTER command, the *outQuery* and *outTotal* counters were always displaying "0". This issue has been resolved.

PCR: 31001 Module: DHCP Level: 2

When executing the SET DHCP POLICY, DELETE DHCP POLICY and DESTROY DHCP POLICY commands, memory was not de-allocated correctly. This issue has been resolved.

PCR: 31002 Module: UTILITY Level: 2

Sometimes the device rebooted when a severe multicast storm occurred due to a loop in the network. This issue has been resolved.

PCR: 31009 Module: HTTP Level: 3

The server string was not copied correctly into an HTTP file request when loading information from the configuration script. This issue has been resolved.

PCR: 31013 Module: SWI Level: 2

If ports were set to a speed of 100m when creating a switch trunk, the speed could not subsequently be set to 1000m, even if the ports were capable of that speed. This issue has been resolved.

PCR: 31015 Module: STP Level: 2

The PORT and PORTPRIORITY parameters of the STP PORT command were not always updating switch instances on ports that are members of multiple STP instances. This issue has been resolved.

PCR: 31017 Module: NTP Level: 3

The *RootDispersion* value in NTP packets was negative. RFC 1305 states that only positive values greater than zero are valid. This issue has been resolved.

PCR: 31019 Module: PIM6 Level: 2

The checksum for the PIMv2 *Register* message for IPv6 was not being calculated correctly. This issue has been resolved.

PCR: 031020 Module: PIM Level: 2

When the switch received a generation ID change message, it was not responding by sending a PIM HELLO message. This issue has been resolved.

PCR: 31028 Module: BGP Level: 2

BGP did not always send *Withdrawn* advertisements when a route went down. This issue has been resolved.

PCR: 31040 Module: PIM Level: 2

When two devices are BSR candidates, and have the same preference set with the SET PIM BSRCANDIDATE PREFERENCE command, the device with the higher IP address was not elected as the candidate. This issue has been resolved.

PCR: 31041 Module: PIM Level: 3

A *Prune* message sent to an old RP neighbour was ignored when a new unicast route was learned. This issue has been resolved.

PCR: 31044 Module: SWI Level: 4

The log message "`IGMP Snooping is active, L3FILT is activated`" has been changed to "`IGMP packet trapping is active, L3FILT is activated`". The revised message is clearer when IGMP is enabled and IGMP snooping is disabled.

PCR: 31052 Module: FIREWALL Level: 3

The following changes have been made to the ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands:

- An IP address range for the IP parameter is now only accepted when enhanced NAT is configured.
- An IP address range for GBLREMOTE parameter is now only accepted when reverse or reverse-enhanced NAT is configured.
- The GBLIP parameter is not accepted for a public interface when enhanced NAT is configured.

PCR: 31058 Module: NTP Level: 3

When the interval between the NTP server and client exceeded 34 years 9 days and 10 hours, the time set on the client was incorrect. This issue has been resolved.

PCR: 31063 Module: IPG Level: 2

MVR was not operating if IGMP had not been enabled. This issue has been resolved.

PCR: 31068 Module: STP Level: 2

A fatal error occurred when the PURGE STP command was executed when STP instances were defined with VLAN members. This issue has been resolved.

PCR: 31071 Module: SWI Level: 4

The warning given when a QoS policy is active on a port operating at reduced speed has been changed to reflect the problem more accurately. The old message was:

```
Warning (2087343): Port <Port num> is currently used in QoS
policy <QoS policy num>, this policy may become incorrect
due to the port bandwidth.
```

The new message is:

```
Warning (2087350): Port <Port num> is operating at less than
its maximum speed: this may affect QoS policy <QoS policy
num>.
```

PCR: 31072 Module: SWI Level: 3

If the DISABLE SWITCH PORT command appeared in the configuration script, an interface could come up even though *ifAdminStatus* was set to 'down'. This issue has been resolved.

PCR: 31080 Module: IPV6 Level: 2

When a ping was sent to the device's link-local address, the device flooded the ICMP *Reply* packet over the VLAN. This issue has been resolved.

PCR: 31081 Module: VRRP, IP, TCP, TELNET, HTTP, SNMP, SSH

This patch adds an enhancement that allows a Virtual Router IP address to be adopted by the current master Virtual Router. This means that regardless of whether the device actually 'owns' the IP address, it will respond to specific service requests made to that IP address. The service requests are ICMP echo (ping), Telnet, SSH, SNMP, HTTP server (GUI), and SSL for the GUI. For details, see "*Adopting the VRRP IP Address*" on page 56.

PCR: 31094 Module: FILE Level: 3

Files with lines over 132 characters in length could not be transferred using TFTP. This limit has now been raised to 1000 characters to match the maximum command line length.

PCR: 31096 Module: FFS Level: 3

The SHOW FILE command caused an error when the displayed file had a duplicate entry due to file size mismatch. This issue has been resolved. An error message is now logged when the SHOW FILE command detects a duplicate file. The first FFS file will be deleted when a duplicate exists.

PCR: 31098 Module: DHCP Level: 3

Static DHCP address ranges were not reclaimed if the *Reclaim* operation was interrupted by the interface going down. This issue has been resolved.

PCR: 31102 Module: DHCP Level: 2

When a boot file for DHCP was specified with the ADD DHCP POLICY FILE command, a blank space was added after the filename in the configuration. This meant the file could not be found. This issue has been resolved.

PCR: 31106 Module: MLD Level: 2

When the device received a version 1 *Query* packet, it become a non-querier on that interface, even if it should have remained as the querier. This issue has been resolved.

PCR: 31118 Module: SWI Level: 2

When the TYPE parameter was specified for the ADD SWITCH L3FILTER command, the type was sometimes a different value in the device's hardware table. This issue has been resolved.

PCR: 31129 Module: IPX2 Level: 2

A fatal error occurred if IPX was disabled and then re-enabled when there was a high rate of incoming IPX traffic on the device. This issue has been resolved.

PCR: 31162 Module: SWI Level: 2

A STP topology change incorrectly deleted static ARP entries. This issue has been resolved.

PCR: 31167 Module: IPG Level: 2

IP MVR member ports were not timing out. MVR member ports now timeout in the same way as IP IGMP ports. The timeout values are configured by IGMP. Also, IGMP interfaces were incorrectly being enabled and disabled by MVR. This issue has been resolved.

Features in 86251-07

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86251-07.

Base Software Release File	86s-251.rez
Patch Release Date	18-Sep-2003
Compressed Patch File Name	86251-07.paz
Compressed Patch File Size	487620 bytes

Patch 86251-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02414 Module: IPV6, SWI, IPG, VLAN

MLD snooping is now supported on AT-9800 Series Switches and Rapier *i* Series Switches. For details, see "*MLD Snooping*" on page 57.

PCR: 03445 Module: IPG

Support has been added for the Ping Polling enhancement. For details, see "*Ping Polling of Device Reachability*" on page 58

PCR: 03524 Module: OSPF, IPG Level: 2

OSPF disabled RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.

PCR: 03530 Module: IPG Level: 2

Running the PURGE IP command with a multicast address and multiple sources was causing a fatal error. This issue has been resolved.

PCR: 03542 Module: HTTP Level: 2

The value specified for the IP parameter in the ADD FIREWALL POLICY PROXY command was not being used by the HTTP proxy. This issue has been resolved.

PCR: 03570 Module: ISAKMP Level: 3

Previously, there was no limit to the number of concurrent ISAKMP Security Associations (SAs), and occasionally new SAs were created until all free memory was exhausted. This issue has been resolved. The number of ISAKMP SAs is now limited to the maximum number of ENCO channels.

Also, if the ISAKMP policy's REMOTEID was set as an X.500 distinguished name (e.g. *ocn=user*), a small amount of memory was consumed by each ISAKMP exchange. This issue has been resolved.

PCR: 03598 Module: ETH, IPG, IPv6, IPX, PORT, PPP. Level: 3

After about 250 days, commands such as SHOW BRIDGE COUNT were not displaying the correct number of seconds for *Uptime* and *Last Change At*. days. This issue has been resolved.

PCR: 03606 Module: IPG Level: 2

BGP and UPNP were not informed when an ETH interface went up or down. This issue has been resolved.

PCR: 03645 Module: OSPF, IPG Level: 2

Directed IPv6 PING messages were being transmitted from other interfaces if the specified interface was down. This issue has been resolved.

PCR: 03734 Module: IPG Level: 2

With static multicasting enabled on two VLANs, only the first few multicast packets of a stream were L3 forwarded. This issue has been resolved.

PCR: 03751 Module: MLDS Level: 3

The MLD snooping entries registered on a port were not removed when the port went down or was unplugged. This issue has been resolved.

PCR: 03764 Module: IPG Level: 3

The IP multicast counter did not increment when IGMP, DVMRP and PIM packets were transmitted and received. This issue has been resolved.

PCR: 03778 Module: FILE, INSTALL, SCR Level: 2

Files used during start up were backed up from NVS to FLASH even if they were already present in FLASH. This used up FLASH memory unnecessarily. This issue has been resolved so that files are only backed up when a copy does not already exist in FLASH.

PCR: 03780 Module: INSTALL Level: 3

If a configuration file had a long file name, the SHOW CONFIG command displayed the file name using the shortened DOS 8.3 format (where file names are 8 characters long, with extensions of 3 characters). This issue has been resolved so that long configuration file names are now displayed using the DOS 16.3 format (where file names are up to 16 characters long).

PCR: 03783 Module: IPG Level: 3

The TIMEOUT and SIZE parameters are only valid for the SET IP DNS CACHE command, but no error message was returned if either parameter was specified for the SET IP DNS command. This issue has been resolved.

PCR: 03784 Module: IPV6 Level: 3

Fragmentation of IPv6 packets now complies with RFC 2460's requirement to align packet sizes to 8 octets.

PCR: 03789 Module: ETH Level: 2

When a 4-port ETH PIC card was installed, the output of the SHOW IP INTERFACE command showed the ETH port as Down, but the link LEDs on the card were lit. This issue has been resolved. The SHOW command now shows the correct link status. The link will go down after 90 seconds if no inbound traffic is received. When inbound traffic is received the link will come up.

PCR: 03796 Module: STP Level: 2

Setting RSTPTYPE to NORMAL, when normal has already been set, sets all ports to the "sending RSTP" state process. This is referred to in IEEE 802.1w as *mCheck*.
When RSTPTYPE was changed from STPCOMPATIBLE to NORMAL with the SET STP command, the STP instance continued to send STP BPDUs until an *mCheck* was performed by entering the SET STP RSTPTYPE=NORMAL command again. This issue has been resolved so that when RSTPTYPE is set to NORMAL an *mCheck* is performed, causing the STP to start sending RSTP BPDUs immediately.

PCR: 03801 Module: MLDS Level: 2

MLD and MLD Snooping accepted MLD *Query* packets with a hop limit greater than 1. Duplicate packets were forwarded when the hop limit was not 1 and the payload was 0::0. This issue has been resolved. MLD and MLD Snooping now require the hop limit to be 1.

PCR: 03802 Module: FIREWALL Level: 1

Packets with bad ACK numbers were sometimes generated by the firewall as part of the proxy TCP setup process. These packets sometimes caused TCP sessions from the public side of the firewall to fail. This issue has been resolved.

PCR: 03809 Module: SWI Level: 2

An additional check has been added for unknown GBIC models to determine if they are copper or fibre.

PCR: 03817 Module: IPV6 Level: 2

A fatal error occurred when IPv6 fragmented a packet. Also, when a large fragmented ICMP echo request packet was received, the reply may not have been fragmented and so may have exceeded the MTU for the interface it was sent on. These issues have been resolved.

PCR: 03823 Module: VLAN Level: 2

If the last port in a VLAN went down, that port was not automatically deleted from IGMP groups. This issue has been resolved.

PCR: 03825 Module: IPG Level: 2

The incorrect logical interface was selected for broadcast packets received with a subnet mask that differed from the class mask. This issue has been resolved.

PCR: 03826 Module: BGP Level: 2

When BGP imported routes from IP with the ADD BGP IMPORT command, and there were multiple import choices, the best IP route was not always imported. This issue has been resolved.

PCR: 03828 Module: IPV6 Level: 2

The MTU value for IPv6 PPP interfaces was always set to 1280 bytes. This MTU value is now correctly set to 1500 bytes, and 1492 bytes for PPP over Ethernet (PPPoE).

PCR: 03836 Module: OSPF Level: 2

OSPF sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03839 Module: IPV6 Level: 2

A fatal error sometimes occurred when an IPv6 ping packet length exceeded 1453 bytes. This issue has been resolved.

PCR: 03841 Module: IPG Level: 2

A fatal error occurred when the PIM path was recovering. This issue has been resolved.

PCR: 03843 Module: DHCP Level: 2

When some DHCP entries were in *Reclaim* mode, and all interface links related to the range of these entries went down, these DHCP entries were stuck in *Reclaim* mode. This issue has been resolved.

PCR: 03850 Module: FFS Level: 3

Files were not displayed in the SHOW FFILE command output, after entering "Q" at the CLI to quit from a previous prompt. This issue has been resolved.

PCR: 03852 Module: IPG, IPV6 Level: 2

PIM SM did not establish a BSR candidate between two AR720 routers with PPP over SYN. This issue has been resolved.

PCR: 03854 Module: SWI Level: 2

When INGRESSLIMIT parameter in the SET SWITCH PORT command was set to 64kbps, the switch received packets intermittently rather than continuously. This issue has been resolved.

PCR: 03855 Module: IPG Level: 2

Previously, an IP multicast stream destined for an IP multicast group was forwarded out ports in the All Groups IGMP snooping entry even after this entry had timed out. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03864 Module: BGP Level: 2

BGP sent *Update* packets when the local host route table changed but did not affect BGP. Also, BGP did not send *Withdrawn* packets when there was a change in the best route. These issues have been resolved.

PCR: 03865 Module: FIREWALL Level: 2

When dual firewall policies were defined, public to private passive mode FTP transfers sometimes failed. This issue has been resolved.

PCR: 03867 Module: BGP Level: 2

BGP sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03870 Module: SWI, VLAN Level: 3

On Rapier 48*i* switches, mirror port information was repeated in the output of the SHOW VLAN command. This issue has been resolved.

PCR: 03875 Module: IPG Level: 2

Sometimes OSPF routes were not entered in the IP route table. This issue has been resolved.

PCR: 03888 Module: DHCP, TELNET Level: 2

When the device was configured as a DHCP server, a fatal error sometimes occurred when a telnet session to the device was closed while DHCP was reclaiming IP addresses. Also, a telnet error message displayed an incorrect value when a telnet command line parameter was repeated (for example, SHOW TELNET TELNET). These issues have been resolved.

PCR: 03896 Module: TTY Level: 3

A fatal error occurred when a long string of text was pasted over an existing long string of text at the CLI. This issue has been resolved.

PCR: 03898 Module: ETH Level: 3

An ETH interface was sometimes shown as *Up* in the output of the SHOW INTERFACE command when it was actually *Down*. This issue has been resolved.

PCR: 03902 Module: FIREWALL Level: 3

Under some circumstances traffic did not have NAT applied if a standard subnet NAT rule was added to a public interface. Such rules did not correctly match incoming traffic when the REMOTEIP parameter in the ADD FIREWALL POLICY RULE command was not specified, and the destination IP address was not the interface's actual IP address. If this situation occurred, traffic was redirected back out the public interface. This issue has been resolved.

PCR: 03906 Module: SWITCH Level: 2

Software emulation of layer 3 hardware filtering was not operating correctly. Packets that the switch had no routing information for were filtered incorrectly. The first packet of a flow that should have been dropped was not dropped, and a flow that should have been allowed was being dropped. This issue has been resolved.

PCR: 03921 Module: IP ARP Level: 3

ARP requests with invalid source MAC and IP addresses were being processed, but should have been dropped. This issue has been resolved.

PCR: 03922 Module: PIM Level: 3

The SET PIM INTERFACE command did not succeed when the HELLOTIMER parameter was specified. This issue has been resolved.

PCR: 03925 Module: IPV6 Level: 3

Incorrect debug information was returned when an ICMPv6 *PacketTooBig* message was received. This issue has been resolved.

PCR: 03928 Module: IKMP Level: 2

ISAKMP in *aggressive* mode did not establish a connection when the peer client sent 10 or more payloads. This issue has been resolved.

PCR: 03931 Module: IPSEC Level: 3

The IPSec configuration was not created correctly when the RADDRESS and LNAME parameters in the CREATE IPSEC POLICY command were used together. This issue has been resolved.

PCR: 03934 Module: IPSEC Level: 2

The CREATE IPSEC POLICY command failed if the interface specified with the INTERFACE parameter did not have a global IPv6 interface defined. This PCR implements a workaround by using the interface's link-local IPv6 address if no other IPv6 address can be found.

PCR: 03936 Module: IKMP Level: 3

When ISAKMP was used with IPv6, an incorrect IP address was displayed in the output of the SHOW ISAKMP EXCHANGE command. This issue has been resolved.

PCR: 03938 Module: IKMP Level: 3

DHEXPONENTLENGTH parameter in the CREATE ISAKMP POLICY command was not accepted when creating ISAKMP policies that used IPv6. This issue has been resolved.

PCR: 03939 Module: IPV6 Level: 2

When a *NeighbourAdvert* message containing an anycast target address was received, the device incorrectly performed Duplicate Address Detection. This issue has been resolved.

PCR: 03946 Module: IPSEC Level: 3

When IPSec was used with IPv6, an incorrect IP address was displayed in the output of the SHOW IPSEC SA command. This issue has been resolved.

PCR: 03949 Module: IPSEC Level: 3

If a local IP address and remote IP address were not specified in the CREATE IPSEC POLICY command for IPv6 IPSec, the SET IPSEC POLICY configuration was shown unnecessarily in the output of the SHOW CONFIG DYNAMIC=IPSEC command. This issue has been resolved.

PCR: 03952 Module: SWI Level: 3

MAC address are now deleted from the all the internal tables for ports where the learn limit has been exceeded.

Features in 86251-06

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86251-06.

Base Software Release File	86s-251.rez
Patch Release Date	30-July-2003
Compressed Patch File Name	86251-06.paz
Compressed Patch File Size	895445 bytes

Patch 86251-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02216 Module: FIREWALL Network affecting: No

Support has been added to the Firewall module for RTSP, MMS, BROBA, and MPEG2.

PCR: 02510 Module: SWI Level: 4

Support has been added for enabling flow control on half duplex links. The ENABLE SWITCH PORT command configures the switch chip to send a jamming signal over a half duplex link in response to congestion. The following commands configure flow control:

```
DISABLE SWITCH PORT={port-list|ALL}
```

```
DISABLE SWITCH PORT=port-list FLOW=PAUSE
DISABLE SWITCH PORT=ALL FLOW={JAMMING|PAUSE}[,...]
ENABLE SWITCH PORT={port-list|ALL}
ENABLE SWITCH PORT=port-list FLOW=PAUSE
ENABLE SWITCH PORT=ALL FLOW={JAMMING|PAUSE}[,...]
SHOW SWITCH PORT[={port-list|ALL}]
```

PCR: 03011 Module: OSPF Network affecting: No

When the router priority was changed on a dynamic OSPF interface, the new priority did not appear in the output of the SHOW OSPF NEIGHBOUR command on neighbouring routers. The new priority only showed after the RESET OSPF command was executed on the neighbouring routers. This issue has been resolved.

PCR: 03070 Module: BGP Level: 2

When BGP imported other route types, it would advertise routes that had nexthops of the BGP peers themselves. The BGP peers would reject these routes and close the peering session, thus preventing the exchange of routing information between BGP peers. This issue has been resolved.

PCR: 03072 Module: BGP Level: 4

The Import parameter of the ADD, SET, DELETE and SHOW BGP commands now has an INTERFACE type. INTERFACE routes were previously grouped with STATIC routes.

PCR: 03178 Module: IPSEC Level: 4

An unnecessary check has been removed from the CREATE ISAKMP POLICY AUTHTYPE=RSASIG command.

PCR: 03264 Module: FIREWALL Level: 4

The event logs for the firewall did not show the correct detail for DOSFLOOD, HOSTSCAN, SYNATTACK and HOSTSCAN. This issue has been resolved.

PCR: 03287 Module: Firewall Level: 2

When the firewall was set to ACTION=NAT, it was allowing inbound traffic, (for example FTP) even though a port was specified for a particular application, (for example Telnet). This issue has been resolved.

PCR: 03310 Module: SWI Level: 3

When the VLAN mirror port was configured as a tagged port, the port did not transmit tagged packets. This issue has been resolved.

PCR: 03315 Module: L2TP Level: 2

The L2TP Framing Type attribute-value pair (19) for virtual tunnels was set to 0 which caused an interoperability problem with a Linux L2TP implementation. This issue has been resolved. The Framing Type attribute-value pair is now set to 1 (synchronous) for virtual tunnels.

PCR: 03355 Module: IPV6 Level: 2

IPv6 tunnelling over IPv4 failed if an IPv4 interface was not configured, even though an IPv4 interface is not needed for IPv6 tunnelling. This issue has been resolved.

PCR: 03374 Module: IPV6 Level: 1

Multilink Listener Discovery (MLD) packets received on the switch caused fatal errors. This issue has been resolved.

PCR: 03425 Module: PRI Level: 3

On the AT-AR020 PRI E1/T1 Port Interface Card (PIC), *E* bits were not transmitted in response to received CRC-4 errors. Also, after a period of Alarm Indication Signal (AIS) reception, Remote Alarm Indication (RAI) transmission was not terminated. These issues have been resolved.

PCR: 03437 Module: IPV6 Level: 2

RIPng received RIP routes from neighbours even when RIPng was disabled. This issue has been resolved.

PCR: 03447 Module: PPP Level: 2

A remotely assigned IP address on a PPP interface was not always released when the connection timed out. This issue has been resolved.

PCR: 03490 Module: IPSEC Level: 2

IPSec used with IPv4 sometimes caused a fatal error. This issue has been resolved.

PCR: 03499 Module: IPG Level: 2

The SET TIME command caused an error on *Refresh* timers for IGMP groups. This issue has been resolved.

PCR: 03511 Module: IPG Level: 3

The special group entry 01-00-5e-00-00-02 was being written to the layer 2 forwarding database to identify router ports for IGMP snooping. Router ports are now identified from software, so this special group entry is no longer written to the layer 2 forwarding database.

PCR: 03514 Module: IPSEC Level: 2

An incorrect IPSec Security Association (SA) was used to transmit packets when the SA's IP address was assigned dynamically on another VPN gateway. This issue has been resolved.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03522 Module: IKMP Level: 3

ISAKMP suffered an error when it encountered unknown cryptographic algorithms. This issue has been resolved.

PCR: 03524 Module: OSPF, IPG Level: 2

OSPF disabled RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.

PCR: 03532 Module: FIREWALL Level: 3

Occasionally the TCP connection was terminated early during an IDENT proxy TCP session. This issue has been resolved.

PCR: 03536 Module: BGP, TCP Level: 3

Outgoing BGP packets did not have the Internet Work control flags set in the IP TOS bits. This issue has been resolved.

PCR: 03537 Module: BGP Level: 3

BGP was returning incorrect and/or incomplete *bgp4AttrPath* MIB entry information. This issue has been resolved.

PCR: 03538 Module: BGP Level: 2

Configuration information was not exported to BGP peers when BGP was disabled and then re-enabled. This issue has been resolved.

PCR: 03543 Module: IPG Level: 2

When acting as a DNS relay agent, the device restarted after approximately three hours of heavy load. This issue has been resolved.

PCR: 03544 Module: HTTP, FIREWALL Level: 3

HTTP proxy was not denying an IP address if its corresponding domain name was specified in a filter, or if a domain name was requested and its corresponding IP address was in the filter. This issue has been resolved.

PCR: 03546 Module: FIREWALL Level: 2

In a dual policy configuration (a LAN policy and a DMZ policy with common WAN interface) where both policies have enhanced NAT, behaviour changed according to which policy was configured first. Traffic received on the WAN interface, where a matching rule existed in the DMZ policy to NAT the traffic through to the DMZ, was not permitted if the DMZ policy was configured first. A deny event was recorded in the LAN policy. The traffic was permitted if the LAN policy was configured first. Also, with the same rule configured when traffic was sent from the LAN interface to the WAN interface, IP traffic through to the DMZ policy did not have NAT applied correctly when the DMZ policy was configured first. An inwards deny event was recorded in the LAN policy. If the LAN policy was configured first this did not occur. Both of these issues have been resolved. In these situations, behaviour is now independent of the order of configuration.

PCR: 03547 Module: DHCP Level: 3

The range of values for the IPMTU parameter in the ADD DHCP POLICY command was set incorrectly in PCR 03465. The correct range is 576-65535, not 579-65535. This issue has been resolved.

PCR: 03551 Module: IPV6 Level: 2

The command ADD IPV6 6TO4 IP did not allow more than one tunnel. This issue has been resolved. This command can now be used repeatedly to create multiple tunnels.

PCR: 03554 Module: FIREWALL Level: 3

When a dynamic public firewall interface was UP it was not possible to delete any (non-dynamic) public interface rules. Also, under the same circumstances it was possible to create duplicates of public interface rules (with the same rule ID number). These issues have been resolved.

PCR: 03555 Module: HTTP Level: 3

The RESET HTTP SERVER command was resetting the dynamic configuration settings back to the default values. This command now resets the HTTP server counters, and restarts the HTTP server using the dynamic configuration settings.

PCR: 03558 Module: PIM, PIM6 Level: 2

Periodic PIM (*,*,RP) *Join* messages did not cease after a set Rendezvous Point timed out. This issue has been resolved.

PCR: 03560 Module: IPV6 Level: 2

A fatal error sometimes occurred when IPv6 multicast packets were forwarded via an interface that went down and then came back up. This issue has been resolved.

PCR: 03562 Module: IPV6 Level: 3

Disabling and then enabling IPv6 made the CREATE IPV6 INTERFACE=VLAN command appear twice in the configuration script. This issue has been resolved.

PCR: 03564 Module: IPV6 Level: 2

A fatal error sometimes occurred when an IPv6 flow used a virtual interface, and the flow was displayed using the SHOW IPV6 FLOW command. This issue has been resolved.

PCR: 03565 Module: BGP Level: 2

A fatal error occurred after executing the SET BGP PEER command when a BGP session was established with more than 15 communities defined. This issue has been resolved.

PCR: 03566 Module: OSPF Level: 2

An area border router did not send summary LSA messages via a PPP link when the area changed. This issue has been resolved.

PCR: 03568 Module: IPV6 Level: 3

IPv6 filters were not handling ICMPv6 packets correctly. This issue has been resolved.

PCR: 03569 Module: FIREWALL Level: 3

A problem existed in a configuration with a single policy involving one private interface and two On Demand PPP public interfaces with NAT acting on traffic from the private to each of the public interfaces. Traffic generated on the device (e.g. pings) that was routed out one of the public interfaces sometimes caused both PPP interfaces to activate. This occurred if the NAT relating to the correct PPP was configured first. This behaviour was partially fixed in PCR 02250. This issue has been resolved so that only one PPP interface is activated and NAT is used correctly.

PCR: 03571 Module: IPG Level: 3

The Proxy Arp default setting should be OFF for VLAN interfaces. This issue has been resolved.

PCR: 03572 Module: STP Level: 4

The *dot1dStpPortForwardTransitions* value in the *dot1dBridge* MIB was not correctly incremented when STP transitioned a port to the forwarding state. This issue has been resolved.

PCR: 03573 Module: IPG Level: 2

It is now possible to configure an IP filter with the default route of 0.0.0.0. This allows BGP to control the default route for route distribution.

PCR: 03574 Module: STP Level: 4

The *dot1dStpInfoTopChanges* value in the *dot1dBridge* MIB was not correctly incremented when a topology change was detected by the bridge. This issue has been resolved.

PCR: 03576 Module: IPG Level: 2

When the device received a route from two separate sources to the same destination network, RIP only used the metric value when selecting the best route. RIP now selects the route by lowest preference value, or if they are the same, by the metric.

PCR: 03582 Module: FIREWALL, IPG Level: 4

Previously, when the ADD FIREWALL POLICY INTERFACE command activated software routing, the static IP ARP entries were removed automatically. Static IP ARP entries now remain and the following message is displayed:

```
WARNING: Static ARPs associated with a particular VLAN are
recommended to be deleted when Firewall is enabled on the VLAN.
```

PCR: 03584 Module: MLD Level: 3

MLD had no mechanism for dealing with an IPv6 interface changing its local link address. This issue has been resolved.

PCR: 03594 Module: PING Level: 2

IPv6 ping or traceroute sometimes caused the device to restart. This issue has been resolved.

PCR: 03609 Module: OSPF Level: 1

The IP route filter did not always work correctly for OSPF. This issue has been resolved.

PCR: 03615 Module: LOAD Level: 3

Zmodem uploads to some terminal emulators did not succeed because the 16-bit checksum was incorrect. This issue has been resolved.

PCR: 03616 Module: IPG Level: 4

Three new commands have been added to enable and disable transmission of the following ICMP messages: *Network Unreachable*, *Host Unreachable,* and all *Redirect* messages.

The commands are:

```
DISABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

ENABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]

SHOW IP ICMPREPLY
```

For details, see "*Enable and Disable ICMP Messages*" on page 60.

PCR: 03618 Module: DHCP Level: 3

The SHOW DHCP CLIENT command output showed a *ClientId* value even when the *State* for the client entry was *Unused*. This issue has been resolved.

PCR: 03619 Module: IPv6 Level: 4

When the SET IPv6 FILTER command specified a filter that did not exist, an `Operation successful` message was displayed as well as an error message. This issue has been resolved.

PCR: 03620 Module: IPV6 Level: 3

The 16-bit reserved field after the maximum response code field was not set to zero, as specified by the Internet Draft *"Multicast Listener Discovery Version 2 (MLDv2) for IPv6"*. This issue has been resolved.

PCR: 03623 Module: SWI Level: 3

If both the EPORT and IPORT parameters were specified with the ADD SWITCH L3FILTER ENTRY command, a value of 63 or 64 for the EPORT parameter was not accepted. This issue has been resolved.

PCR: 03624 Module: IPV6 Level: 3

The ADD IPV6 FILTER and SET IPV6 FILTER commands accepted a SESSION parameter when the PROTOCOL parameter was not TCP. The SESSION parameter specifies the type of TCP packet to match. This issue has been resolved.

PCR: 03625 Module: STP, SWI Level: 4

The MIB object *dot1dStpTimeSinceTopologyChange* has been implemented to record when a topology change is detected by the bridge.

PCR: 03631 Module: SWI Level: 4

When a Finisar 8521 GBIC was used in an AT-A42/GBIC uplink module the link LED did not correctly show the link status. This issue has been resolved.

PCR: 03635 Module: IPV6 Level: 1

IPv6 was selecting routes on interfaces that were down. This issue has been resolved.

PCR: 03637 Module: IPV6 Level: 1

IPv6 static tunnels remained in the Tentative state and did not change to the Preferred state. This issue has been resolved.

PCR: 03640 Module: STP Level: 2

A fatal error sometimes occurred when the ENABLE STP PORT command was executed. This issue has been resolved.

PCR: 03646 Module: IPv6 Level: 1

A fatal error occurred when the SHOW IPV6 MLD INTERFACE command was executed after the interface had been destroyed. This issue has been resolved.

PCR: 03647 Module: SNMP Level: 2

A fatal error occurred when a *Set* request with an incorrect object ID value was received by SNMPv2c. This issue has been resolved.

PCR: 03650 Module: IPG Level: 3

IGMP *Query* messages were sent over an interface even if IGMP had been disabled on that interface. This issue has been resolved.

PCR: 03652 Module: SWI Level: 2

Packet forwarding between switch chips on Rapier 48 switches sometimes failed if ingress rate limiting was set below 1 Mb/s. This was caused by packets receiving a bad hop count between switch chips via the CPU, causing packets to be discarded. This issue has been resolved.

PCR: 03657 Module: SWI Level: 3

Executing the DISABLE SWITCH PORT command on a port that was the source of a mirror port did not disable the mirror port. This issue has been resolved.

PCR: 03662 Module: IPG Level: 1

Equal Cost Multi-Path (ECMP) routing selected a route with an infinite metric, so that forwarded packets using that route were discarded. This issue has been resolved.

PCR: 03666 Module: BGP Level: 3

BGP advertised interface routes when the corresponding interface was down. This issue has been resolved.

PCR: 03669 Module: FIREWALL Level: 3

If the firewall received a packet with an incorrect TCP checksum and ACK number, the packet was sent to the client. Such packets are now rejected by the firewall. This patch fixes the problem.

PCR: 03678 Module: IPG Level: 3

Packet throughput was reduced if an incoming packet did not match the first entry of the IP filter table. This issue has been resolved.

PCR: 03679 Module: IPG Level: 3

When IP filters were deleted, the corresponding IP flow cache was not invalidated. This issue has been resolved.

PCR: 03689 Module: PKI Level: 1

A fatal error occurred when a device received a PKI certificate that exceeded the CERTSTORELIMIT parameter in the SET PKI command. This parameter sets the maximum number of certificates that can be stored on the device. This issue has been resolved.

PCR: 03691 Module: DVMRP Level: 2

A fatal error occurred if the number of DVMRP interfaces being added exceeded the limit. This issue has been resolved.

PCR: 03692 Module: BGP Level: 2

Occasionally a fatal exception may have occurred when sending BGP aggregate routes. This issue has been resolved.

PCR: 03696 Module: IPG Level: 2

IGMP snooping entries were not being deleted from the hardware table. This issue has been resolved. Also, port timers are now updated when the IGMP timeout is changed.

PCR: 03698 Module: DVMRP Level: 3

The output of the SHOW DVMRP FORWARDING command did not display the forwarding ports. This issue has been resolved.

PCR: 03707 Module: STP Level: 2

When adding a port to a VLAN, any STP ports that had been disabled in the default STP were re-enabled. This issue has been resolved.

PCR: 03708 Module: DHCP Level: 2

When the DELETE DHCP RANGE command was executed, DHCP attempted to reclaim the addresses in that range. It also tried to reclaim addresses in that range that were not allocated at that time, resulting in duplicate addresses appearing on the free list for allocation. This has been resolved by allowing DHCP to reclaim only those addresses that are currently in use by one of its clients.

PCR: 03710 Module: PIM, PIM6 Level: 2

The list of multicast groups for each Rendezvous Point occasionally became corrupted, and this could cause a fatal error. This issue has been resolved.

PCR: 03720 Module: STP Level: 2

When changing from RSTP to STP mode, the STPCOMPATIBLE option for the RSTPTYPE parameter incorrectly appeared in the dynamic configuration. Also, when changing from RSTP to STP mode or vice versa, disabled STP ports did not remain in the disabled state. These issues have been resolved.

PCR: 03722 Module: PPP, VJC Level: 3

Previously, VJC supported 136 interfaces and PPPoE supported 256 PPP interfaces, but the device software supported up to 512 PPP interfaces. This discrepancy sometimes caused a fatal error and prevented PPPoE interfaces with a PPP index greater than 255 from working correctly. This issue has been resolved, so that VJC and PPPoE now fully support 512 PPP interfaces.

PCR: 03723 Module: BGP Level: 2

BGP routes that were added after a summary aggregate route had been formed were not suppressed. This issue has been resolved: all routes added after summary aggregate route creation are also now suppressed.

The SHOW BGP ROUTE command displayed unselected routes as the "best" route, until they had been processed. This issue has been resolved.

When a single route was deleted from an aggregate route, the aggregate route was deleted, even if it contained other routes. This issue has been resolved.

PCR: 03728 Module: IPG Level: 4

A field has been added to the SHOW IP command output that displays whether the IP ARP log is enabled or disabled.

PCR: 03733 Module: IPV6 Level: 3

When an oversize packet (PMTU) was received, an error message was not returned, even when IPv6 flow was enabled. This issue has been resolved.

PCR: 03738 Module: IPG Level: 2

If a port went down, the port was deleted from the appropriate static IGMP associations but was not added back again when it came back up. Similarly, static IGMP associations were automatically deleted but not added back when IP or IGMP was disabled. These issues have been resolved. You can now create IGMP associations before enabling IGMP, and they will become active when IGMP is enabled.

PCR: 03741 Module: FIREWALL Level: 3

The maximum number of firewall sessions had decreased since software release 86s-241. This issue has been resolved.

PCR: 03743 Module: IP Level: 3

If a ping was active and the IP configuration was reset, subsequent pings were sent out the wrong interface. This issue has been resolved.

PCR: 03744 Module: PING Level: 3

Executing a ping to the IP address 0.0.0.0 did not return an `invalid destination address` error message. Also, when the TRACE command was executed for local addresses, it timed out after 90 seconds. These issues have been resolved.

PCR: 03747 Module: VRRP Level: 3

An *unkown interface* log message was returned for VRRP if there was an interface UP or interface DOWN event due to a mismatch between a monitored interface index and the corresponding interface instance. This issue has been resolved.

PCR: 03750 Module: IPv6 Level: 3

IPv6 loopback address was used as a source address in ping packets, causing ping to fail. This issue has been resolved.

PCR: 03756 Module: IPV6 Level: 2

The following issues have been resolved:

- IPv4 addresses x.x.x.0 or x.x.x.255 were not accepted for the IP parameter in the ADD IPV6 6TO4 command.
- IPv4 addresses x.x.x.0 or x.x.x.255 were not accepted for the LOCAL parameter in the ADD IPV6 TUNNEL command.
- IPv6 addresses 2002:x:x::/48 were not accepted for the IPADDRESS parameter in the ADD IPV6 INTERFACE command.

PCR: 03766 Module: FIREWALL Level: 2

The firewall denied streaming data using Windows Media Player 9. This issue has been resolved.

PCR: 03771 Module: SWI Level: 2

When ingress rate limiting was used on Rapier switch ports, TCP sessions sometimes obtained a throughput that was lower than the configured ingress rate limit. This issue has been resolved.

PCR: 03790 Module: SWI Level: 2

When a tagged port was deleted from a VLAN that was in the default STP, and the port was then added to the VLAN again, communications were sometimes not resumed on that port. This issue has been resolved.

PCR: 03793 Module: RSVP Level: 3

The ENABLE RSVP INTERFACE command did not succeed if IP was enabled after the RSVP interface had been created. Now, ENABLE RSVP INTERFACE will succeed regardless of when IP is enabled as long as an IP interface exists.

Features in 86251-05

Patch file details are listed in Table 4:

Table 4: Patch file details for Patch 86251-05.

Base Software Release File	86s-251.rez
Patch Release Date	15-May-2003
Compressed Patch File Name	86251-05.paz
Compressed Patch File Size	320764 bytes

Patch 86251-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02583 Module: FIREWALL Level: 2

UDP packets passed through the firewall by a reverse enhanced NAT rule were getting an incorrect IP checksum. This caused IP to discard the packets. This issue has been resolved.

PCR: 03059 Module: FIREWALL Level: 2

SMTP proxy was falsely detecting third party relay under some circumstances. This issue has been resolved.

PCR: 03095 Module: DHCP Level: 2

DHCP policies are no longer stored in alphabetical order in the DYNAMIC CONFIGURATION script because this did not work when the DHCP INHERIT parameter was used.

PCR: 03148 Module: IPG Level: 3

If the Gratuitous ARP feature was enabled on an IP interface, and an ARP packet arrived, (either ARP request, or reply) that had a Target IP address that was equal to the SenderIP address, then the ARP cache was not updated with the ARP packet's source data. This issue has been resolved.

PCR: 03177 Module: IPG Level: 3

Deleting an IP MVR group range would only delete the last IP address of the range from the multicast table, not the entire range. This issue has been resolved.

PCR: 03199 Module: IPV6 Level: 3

RIPng was receiving invalid routes and packets. This issue has been resolved.

PCR: 03241 Module: FIREWALL Level: 3

When deleting a list associated with a policy, all rules were being deleted. Now only the rules associated with the policy and list are deleted.

PCR: 03270 Module: SWI Level: 3

The inter-packet gap has been reduced by 4 bytes on the Rapier 48*i* stacking link. This allows for non-blocking operation with tagged packets.

PCR: 03299 Module: IKMP Level: 2

Under some circumstances, ISAKMP suffered a fatal error if more than 8 SA proposals were presented. This issue has been resolved.

PCR: 03314 Module: SWI Level: 2

Layer 3 filters that matched TCP or UDP port numbers were being applied to the second and subsequent fragments of large fragmented packets. This issue has been resolved.

PCR: 03354 Module: FIREWALL Level: 3

The SET FIREWALL POLICY RULE command was not accepting the value 24:00 (midnight) for the BEFORE parameter. This issue has been resolved.

PCR: 03371 Module: DHCP Level: 3

A minimum lease time can no longer be specified when creating a DHCP policy. This complies with RFC 2131.

PCR: 03383 Module: IPG Level: 2

If there were a large number of routes in the route table, and the SHOW IP ROUTE command was executed, the device stopped operating. This issue has been resolved.

PCR: 03390 Module: HTTP Level: 2

Occasionally a fatal error occurred when the GUI browser started or a page was refreshed. This issue has been resolved.

PCR: 03392 Module: IPSEC, IKMP Level: 3

IPV4 is the default for the IPVERSION parameter in the CREATE IPSEC POLICY and CREATE ISAKMP POLICY commands. This default was unnecessarily displayed in the SHOW CONFIGURATION DYNAMIC command output. This issue has been resolved.

PCR: 03395 Module: BGP Level: 3

The amount of time that BGP peers 'back off' for after changing from the ESTABLISHED state to the IDLE state has been changed. Previously, this 'back off' time grew exponentially and never decayed. The 'back off' time is now always one second.

PCR: 03396 Module: ETH Level: 3

Some memory was lost on the AT-AR022 ETH PIC when hotswapping. This issue has been resolved.

PCR: 03400 Module: SSL Level: 3

Sometimes SSL did not allow its TCP session to close properly. This happened if the *Fin* packet was not piggy-backed on a data packet, or if the SSL Handshake was never completed with the far end. This meant that the closing *Alert* was not sent, so the session could not close. Also, SSL leaked memory when it received invalid SSL records. These issues have been resolved.

PCR: 03402 Module: IPG Level: 2

IP routes deleted from the route cache occasionally caused a fatal error. This issue has been resolved.

PCR: 03405 Module: STREAM Level: 2

The reconnection to the stream printing TCP port failed after a single successful connection was made. This issue has been resolved.

PCR: 03407 Module: IPG Level: 3

The default for the PROXYARP parameter in the SET IP INTERFACE command for a VLAN interface was OFF. The default is now ON.

PCR: 03410 Module: VLAN, CORE Level: 3

If a patch was running with a major software release, after a VLAN was added at the command line, the VLAN was not shown as UP. This issue has been resolved.

PCR: 03412 Module: FIREWALL Level: 3

FTP data transfers did not succeed for some types of NAT. Also, the presence of flow control TCP flags meant that some TCP control packets were not recognised. These issues have been resolved.

PCR: 03413 Module: BGP Level: 2

BGP was updated according to the most recently added route. BGP now updates to reflect the best available route, regardless of when it was added.

PCR: 03415 Module: FIREWALL Level: 2

When using a policy routing rule, the firewall did not translate the source IP address of a broadcast packet correctly. This issue has been resolved.

PCR: 03416 Module: SWI Level: 3

Previously, the ADD SWITCH L3FILTER MATCH command was accepted if the TYPE parameter was not specified. This command now requires the TYPE parameter, and an error message will be returned if the TYPE parameter is not specified.

PCR: 03424 Module: DHCP Level: 2

When static DHCP was set to the first IP address in a range, that range would stay in the *Reclaim* mode. This issue has been resolved.

PCR: 03426 Module: IPV6 Level: 3

If the valid and preferred lifetimes of an IPv6 address for a given interface were set to infinity, they were not included in the dynamic configuration. This issue has been resolved.

PCR: 03429 Module: SWI, VLAN Level: 3

The SHOW VLAN command was displaying a port that did not exist. This issue has been resolved.

PCR: 03430 Module: BGP Level: 3

BGP traps were sent incorrectly when a BGP peer became Established, or moved into a lower state. This issue has been resolved.

PCR: 03432 Module: STP Level: 2

STP settings were not retained when a port was deleted from the VLAN that the STP belongs to. This issue has been resolved.

PCR: 03436 Module: IP, DHCP Level: 2

When the device was acting as a DHCP client and the DHCP server provided a gateway address, a statically configured default route was deleted and replaced with a default route with the provided gateway address. The correct behaviour is to only delete a dynamic default route in this situation. This issue has been resolved; the correct behaviour is now applied.

PCR: 03439 Module: IPX Level: 3

The IPX traffic filter match counter was not incremented if a route was cached. This issue has been resolved.

PCR: 03441 Module: L2TP Level: 2

PPP configured on a L2TP access concentrator (LAC) should be dynamic. If PPP was incorrectly configured to be static, the static PPP was destroyed when the L2TP tunnel was formed so that only the first connection succeeded. This issue has been resolved so that an L2TP tunnel is not created if the PPP is static.

PCR: 03443 Module: DHCP Level: 3

When a DHCP entry expired while other DHCP entries in the range were in *Reclaim* mode, unnecessary ARP packets were generated causing an ARP storm. This issue has been resolved.

PCR: 03444 Module: FR Level: 3

The CIR and CIRLIMITED parameter in the SET FRAMERELAY DLC command now regulates the behaviour of the transmission rate. Previously, the transmission rate did not reflect changes to the CIR setting if the new CIR was higher than the old CIR (provided that the new CIR is within the physical maximum of the network and the hardware), or changes to the CIRLIMITED setting if CIRLIMITED was turned ON then OFF. This issue has been resolved.

PCR: 03446 Module: SWI Level: 3

After unplugging a fibre uplink cable and then plugging it back in, a short Ping timeout occurred. This issue has been resolved.

PCR: 03450 Module: PIM, PIM6 Level: 2

Receiving PIM *State Refresh* messages now creates and/or maintains PIM forwarding information.

PCR: 03453 Module: FIREWALL Level: 3

The dropped packets counter for the firewall was not incrementing correctly. This issue has been resolved.

PCR: 03454 Module: IPV6 Level: 3

Occasionally, removing the cable from an IPv6 interface caused the device to stop responding. This issue has been resolved.

PCR: 03456 Module: PIM Level: 2

A VLAN interface receiving a PIM *Prune* message on a port stopped forwarding multicast data to that port too early. This could cause multicast data to arrive after a PIM *Prune*, so an override PIM *Join* message was not sent, leading to a loss of multicast data. This issue has been resolved.

PCR: 03457 Module: OSPF Level: 2

Disabling OSPF caused a fatal error if there was a large routing table. This issue has been resolved.

PCR: 03459 Module: IPV6 Level: 2

A fatal error sometimes occurred when packets were forwarded via an IPv6 interface, and IPv6 flows were disabled. This issue has been resolved.

PCR: 03461 Module: IPG Level: 3

The ENABLE IP MVR DEBUG=ALL command was erroneously shown in the output of the SHOW CONFIG DYNAMIC=IP command. This SHOW output no longer includes the ENABLE IP MVR DEBUG=ALL entry.

PCR: 03462 Module: PIM, PIM6 Level: 3

PIM *Graft* and *Graft-Ack* counters were not incrementing. This issue has been resolved.

PCR: 03465 Module: DHCP Level: 3

The IPMTU parameter in the ADD DHCP POLICY command was accepting values in the range 0-4294967295. This parameter now accepts values in the correct range of 579-65535.

PCR: 03463 Module: PIM, PIM6 Level: 3

PIM-SM *Null* register messages did not update the register counter correctly, and did not trigger *Register* debug messages. This issue has been resolved.

PCR: 03464 Module: PIM, PIM6 Level: 3

PIM-SM *Null* register messages for non-PIM-SM domain sources did not have the *Border* bit set. This issue has been resolved.

PCR: 03467 Module: IPG Level: 3

An invalid message appeared when the PORT parameter was specified for the ADD IP ROUTE command. This issue has been resolved.

PCR: 03471 Module: IPV6 Level: 2

A fatal error sometimes occurred when forwarding traffic over an IPv6 tunnel. This issue has been resolved.

PCR: 03473 Module: PIM, PIM6 Level: 3

The SET LAPD MODE=NONAUTOMATIC command did not change the LAPD mode from automatic to non-automatic. This issue has been resolved.

PCR: 03474 Module: FIREWALL Level: 3

The SMTP proxy did not correctly allow outgoing (private to public) SMTP sessions when the DIRECTION parameter was set to OUT or BOTH in the ADD FIREWALL PROXY command. This issue has been resolved.

PCR: 03475 Module: NTP Level: 3

The PURGE NTP command did not change the UTC offset to the initialised value. This issue has been resolved.

PCR: 03476 Module: IPV6 Level: 3

RIPng was showing routes to interfaces that were DOWN as being UP. This issue has been resolved.

PCR: 03478 Module: PIM, PIM6 Level: 3

The message format for PIM-SM periodic (*,*,RP) *Join* messages was incorrect when the message contained more than one joined RP address. This issue has been resolved.

PCR: 03484 Module: FIREWALL Level: 3

The firewall was not denying an ICMP packet, even if ICMP Forwarding was disabled when using Standard NAT. This issue has been resolved.

PCR: 03492 Module: HTTP, LOAD Level: 2

Some memory loss occurred when loading a file via HTTP. This issue has been resolved.

PCR: 03494 Module: BGP, FIREWALL Level: 2

If the firewall was enabled when BGP was in use outgoing BGP data packets would have IP header errors and incorrect checksums. This problem has now been fixed.

PCR: 03497 Module: PIM, PIM6 Level: 2

In a network with an alternative path, if the link connected to the interface where a Candidate Rendezvous Point (CRP) advertised its RP candidacy was down, the CRP did not re-advertise its RP candidacy on other available interfaces (the alternative path). This meant that the CRP did not update its PIM routes, which was necessary to re-establish the PIM tree in order for multicast data to flow again. This issue has been resolved.

PCR: 03498 Module: SWI Level: 3

The SHOW SWITCH FDB command showed a number of irrelevant entries. This issue has been resolved.

PCR: 03502 Module: IPG Level: 3

The ENTRY parameter from the ADD IP FILTER command was not included in the output of the SHOW CONFIG DYNAMIC command. This issue has been resolved.

PCR: 03513 Module: IPG Level: 3

An enhancement allows for the creation of static IGMP group memberships that do not time out. For details on this feature, see "*Static IGMP*" on page 62.

PCR: 03515 Module: DHCP Level: 3

DHCP was offering network and broadcast addresses to clients. This issue has been resolved.

PCR: 03517 Module: FIREWALL Level: 3

An error was not returned if the SET FIREWALL POLICY RULE command was executed with PROTOCOL=1 when ICMP forwarding was turned on. This issue has been resolved so that an error is now displayed.

PCR: 03523 Module: FIREWALL Level: 2

In some circumstances the checksum for the TCP header was set to zero. This issue has been resolved.

PCR: 03526 Module: SWI Level: 3

The Switch MIB did not show the correct *dot1StpPriority* value. This issue has been resolved.

PCR: 03531 Module: SWI Level: 3

After creating a trunk group, the activity LEDs did not flash unless the configuration was used at reboot. This issue has been resolved so that the LEDs flash correctly whenever a trunk group is created.

PCR: 03468 Module: PIM Level: 3

The source IP address in a PIM *Register* message was not the DR interface's IP address. This issue has been resolved.

PCR: 03533 Module: PIM Level: 3

A forwarded PIM-DM state *Refresh* message did not update the metric and preference values. This issue has been resolved.

PCR: 03535 Module: IPG Level: 2

IGMP *Query* messages were not sent after IGMP was disabled and then re-enabled. This issue has been resolved.

Features in 86251-04

Patch file details are listed in Table 5:

Table 5: Patch file details for Patch 86251-04.

Base Software Release File	86s-251.rez
Patch Release Date	15-April-2003
Compressed Patch File Name	86251-04.paz
Compressed Patch File Size	240936 bytes

Patch 86251-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02571 Module: IP Level: 3

A fatal error occurred if the IP module was reset after the ADD IP EGP command was executed. This issue has been resolved.

PCR: 02577 Module: IPG, LOG Level: 4

The ability to log MAC addresses whenever the ARP cache changes has been added. To enable this, use the command:

```
ENABLE IP ARP LOG
```

To disable it, use the command:

```
DISABLE IP ARP LOG
```

The logging of MAC addresses is disabled by default. Use the SHOW LOG command to view the MAC addresses that have been logged when the ARP cache changes.

PCR: 03025 Module: GUI Level: 2

A buffer address was incrementing and not returning buffers for reuse when the command line interface was accessed via the GUI interface. This issue has been resolved.

PCR: 03044 Module: BGP Level: 2

During route flapping, peers were sometimes not told about routes to the same destinations as the flapping routes. This issue has been resolved.

PCR: 03048 Module: STP Level: 2

If a port belongs to an enabled STP instance, but the port has been disabled from STP operation with the DISABLE STP PORT command, the port will not respond to ARP requests. This patch implements a workaround that allows disabled STP ports to respond to ARP requests.

PCR: 03089 Module: CORE Level: 4

The SET SYSTEM NAME command was accepting character strings greater than the limit of 80 characters. This issue has been resolved.

PCR: 03094 Module: STP, VLAN Level: 3

The VLAN membership count for STP ports was incorrect in the default configuration. This issue has been resolved.

PCR: 03096 Module: VLAN Level: 2

OSPF and RIP *Hello* packets were being sent out all trunked ports. Now these *Hello* packets are only sent out the master port of the trunked group.

PCR: 03097 Module: IPV6 Level: 3

A device could not Telnet to a device outside its own subnet. This issue has been resolved.

PCR: 03098 Module: PIM, DVMRP, IPG Level: 2

When multicasting in hardware, the switch would not forward packets from a VLAN ingress interface to a non-VLAN interface downstream. This issue has been resolved.

PCR: 03105 Module: FIREWALL Level: 3

Incorrect handling of TCP sessions, and poor load balancing performance could be caused by TCP virtual balancers not selecting a new resource if required. This issue has been resolved.

PCR: 03109 Module: LOG Level: 3

A log was only partially created if there was insufficient NVS memory for log creation on the router. A change has been made so that a log is not created if there is insufficient memory, and a warning message is displayed.

PCR: 03110 Module: IPG Level: 3

An error occurred with the ADD IP MVR command. This issue has been resolved. Also, this command accepted any IP addresses for the GROUP parameter, but now only accepts multicast addresses.

PCR: 03111 Module: FIREWALL Level: 1

TCP sessions could fail if the public side of the firewall was using Kerberos and the private side had a very slow connection to the firewall. This issue has been resolved.

PCR: 03115 Module: PING Level: 3

The SHOW CONFIG DYNAMIC=PING command was giving an incorrect port number. This issue has been resolved.

PCR: 03116 Module: FIREWALL Level: 2

An error sometimes occurred in the firewall module under heavy FTP or RTSP traffic loads. This issue has been resolved.

PCR: 03117 Module: FIREWALL Level: 1

The TCP sequence numbers are no longer altered through the firewall when TCPSETUP is disabled with the DISABLE FIREWALL POLICY command.

PCR: 03119 Module: CLASSIFIER Level: 4

TCP source and TCP destination ports were swapped when viewed in the GUI. This issue has been resolved.

PCR: 03120 Module: ETH, IPG Level: 4

The SHOW IP INTERFACE command was showing ETH interfaces as up at startup, when SHOW INTERFACE and SHOW ETH STATE had them as down. This issue has been resolved.

PCR: 03124 Module: IPV6 Level: 4

The SHOW IPv6 COUNTER command now shows the *outAdvert* messages in the Total Out Messages counter field.

PCR: 03132 Module: SWITCH Level: 2

Classifiers that were added to hardware filters were not applied to the hardware. This issue has been resolved.

PCR: 03139 Module: IPV6 Level: 3

The SHOW IPV6 INTERFACE command was not displaying the link layer address and EUI when the interface was down. This issue has been resolved.

PCR: 03140 Module: IPG, SWI Level: 2

Static ARPs were deleted when a port went down. This issue has been resolved.

PCR: 03144 Module: CURE Level: 4

Users with either USER or MANAGER level privilege can now execute the STOP PING and STOP TRACE commands. Previously, MANAGER privilege was needed to execute these commands.

PCR: 03145 Module: IPG Level: 4

The SET IP ROUTE FILTER command was not processing some parameters. This issue has been resolved.

PCR: 03146 Module: PORT Level: 4

The PAGE parameter in the SET ASYN command now only accepts numeric values between 0 and 99, ON or OFF, and TRUE or FALSE.

PCR: 03147 Module: BGP Level: 4

When the DISABLE BGP DEBUG command was used, debugging messages were still being displayed by the BGP module. This issue has been resolved.

PCR: 03149 Module: SWITCH Level: 3

When the Layer 3 Filter Match entry IMPORT was created, EPORT could be set on the filter entry. If the Layer 3 Filter Match entry EMPORT was created, then IPORT could be set on the filter entry. Setting parameters that did not match could cause undesirable results. This issue has been resolved.

PCR: 03150 Module: FIREWALL Level: 3

The CREATE FIREWALL POLICY command was not checking for valid name entries, so invalid printing characters could be used for policy names. This issue has been resolved.

PCR: 03152 Module: IPG Level: 3

An additional check has been added to validate the MASK specified in an ADD IP ROUTE command. The check tests that the mask is contiguous.

PCR: 03153 Module: ACC Level: 4

The SHOW CONFIG=ACC command was not showing the *rscript* file. This issue has been resolved.

PCR: 03154 Module: PCI Level: 4

The SHOW IP MVR command output was showing dynamic members in the incorrect column. This issue has been resolved.

PCR: 03155 Module: FFS Level: 4

The SHOW FFILE command output has changed. The first column that listed where the file was stored has been removed. The title of the original second column (now the first column) has been changed from “creator” to “module”. The file format specifier has been altered from:

DDDD:MMMM\NNNNNNNN.TTT

to:

MMMM\NNNNNNNN.TTT

PCR: 03157 Module: IPV6 Level: 3

When changing the ACTION parameter between INCLUDE and EXCLUDE on IPV6 filters the interface information was not preserved between changes. The interface information is now preserved.

PCR: 03159 Module: SWI Level: 2

Switch trunk speed checks only checked for gigabit settings, not speed capabilities. It is now possible for uplink modules which support 10, 000 and gigabit speed to attach to trunks where speeds are 10Mb/s or 100Mb/s.

PCR: 03162 Module: IPV6 Level: 3

The performance of IPv6 has been improved by introducing IPv6 flows.

PCR: 03163 Module: IPG Level: 3

IGMP Snooping did not use DVMRP messages to identify a port. This issue has been resolved.

PCR: 03166 Module: IPG Level: 4

The output of the SHOW IP IGMP COUNTER and SHOW IGMPSNOOPING COUNTER commands was incorrect. This issue has been resolved.

PCR: 03167 Module: DVMRP Level: 2

When multicasting to a VLAN interface, if more than 2 DVMRP neighbours existed on a single port, and any one of those neighbours was pruned, the multicast data would stop flowing to the port. This happened even though it was still required for the remaining DVMRP neighbours. This issue has been resolved.

PCR: 03169 Module: IPV6 Level: 2

Duplicate Address Detection (DAD) was not sent on VLAN interfaces. This issue has been resolved.

PCR: 03180 Module: IPG Level: 3

If all 32 VLAN interfaces had IP addresses attached, only 31 VLANs could be multihomed. Now all 32 VLAN interfaces with IP addresses can be multihomed.

PCR: 03186 Module: CORE, FFS, TTY Level: 3

When the QUIT option was chosen after the SHOW DEBUG command was executed, the output did not immediately stop. This issue has been resolved, but there may be a short delay before the command prompt reappears.

PCR: 03187 Module: IPG Level: 3

SNMP *linkup* traps were not all appearing due to too many outstanding ARP requests. This issue has been resolved. IP now does not limit the number of outstanding ARP requests.

PCR: 03189 Module: FIREWALL, LB Level: 3

A fatal error occurred for the load balancer when there were no UP resources in a resource pool. This issue has been resolved. Load balanced TCP connections will now only retry SYNs once after 5 seconds. The round robin selection algorithm will now select an UP resource in a resource pool with only one UP resource, even if it was used for the last successful connection.

PCR: 03194 Module: LB Level: 3

Sometimes healthcheck pings were not sent to the load balancer resources. This issue has been resolved.

PCR: 03195 Module: USER Level: 3

When a user was logged in as MANAGER, and Telnet was set to OFF, and the CREATE CONFIGURATION command was executed, Telnet would be reset to ON on startup. This issue has been resolved.

PCR: 03196 Module: IPV6 Level: 3

The system became unstable if the ADD IPV6 TUNNEL command failed. This instability was caused by the partially created tunnel entry not being properly removed from the tunnel database. The tunnel entry is now completely removed.

PCR: 03198 Module: PRI Level: 3

The PRI interface would occasionally take a long time for the ifOperStatus of the interface to become UP. This issue has been resolved.

PCR: 03203 Module: IPV6 Level: 3

RIPng was not sending a response back to a RIP request message. This issue has been resolved.

PCR: 03205 Module: DHCP Level: 2

The following issues with DHCP have been resolved:

- DHCP assigned an incorrect IP address to clients shifting from a relayed to a non-relayed range. Gateway checks have been added to resolve this issue.
- DHCP clients shifting between relayed ranges were not always recognised, and were occasionally allocated incorrect addresses.
- DHCP offered entries did not time out after a NAK on a bad lease time request.

PCR: 03206 Module: IPG Level: 3

IPv4 filters now behave like IPv6 filters.

PCR: 03208 Module: FIREWALL Level: 2

When the configuration script was created using the CREATE CONFIG command, the GBLIP parameter in the ADD FIREWALL POLICY command was listed twice. This caused the command to fail when the device was restarted. This issue has been resolved.

PCR: 03211 Module: SWI Level: 2

When the MARL table had been fully populated, the addition of another multicast group caused an entry to be deleted, and the new entry was not added. This issue has been resolved so that no more groups can be added when the table is full.

PCR: 03212 Module: IPV6 Level: 3

The TRACE command was not working when using an ipv6 link-local address. This issue has been resolved.

PCR: 03213 Module: IPSEC Level: 3

A memory leak occurred when some IPSEC processes failed. This issue has been resolved.

PCR: 03216 Module: PIM, PIM6 Level: 2

PIM4 and PIM6 were not sending Hello packets if the HELLOINTERVAL was not a multiple of 10. This is set with the ADD PIM INTERFACE, ADD PIM6 INTERFACE, SET PIM INTERFACE, and SET PIM6 INTERFACE commands. This issue has been resolved.

PCR: 03222 Module: PIM, PIM6 Level: 2

If the RP candidate advertising time was set to a non-default value with the ADVINTERVAL parameter in the SET PIM command, the hold time in the message was not being updated correctly. This issue has been resolved.

PCR: 03229 Module: LOAD Level: 3

Zmodem was not naming some loaded files. This issue has been resolved.

PCR: 03232 Module: BGP Level: 3

Values for the KEEPALIVE and HOLDTIME parameters in the ADD BGP PEER and SET BGP PEER commands were not interacting correctly. This issue has been resolved.

PCR: 03234 Module: IPG Level: 3

The PURGE IP command did not remove ENABLE IP IGMP from the configuration. This issue has been resolved.

PCR: 03236 Module: IPG Level: 3

IGMP queries were being sent after IGMP was disabled. This issue has been resolved.

PCR: 03237 Module: IPG Level: 2

RIP *Request* packets for IPv4 were not being transmitted when the link came up or when the switch restarted. This issue has been resolved.

PCR: 03238 Module: SWI Level: 2

When RIP interfaces were deleted, the IP routes learned through those interfaces were not timing out correctly. Now, all IP routes learned though a RIP interface are removed when the RIP interface is deleted, and no timeouts occur.

PCR: 03239 Module: QOS Level: 2

QoS Traffic Class maximum bandwidth limiting was being overwritten by the port or trunk maximum bandwidth value. This should only happen when the Traffic Class maximum bandwidth has *not* been set manually with the CREATE QOS TRAFFICCLASS MAXBANDWIDTH parameter. This issue has been resolved.

PCR: 03240 Module: OSPF Level: 2

A fatal error occurred when OSPF was under high load. This issue has been resolved.

PCR: 03245 Module: SWI, IPG, PIM Level: 2

Multicast streams would not commence forwarding immediately due to IGMP packets initiated but not sent while a VLAN was changing from the DOWN to UP state. Also, multicast streams could be received while the VLAN was changing from DOWN to UP, causing a PIM Reverse Path Forwarding unicast route lookup failure. This was due to the unicast route being unusable as the VLAN was still considered down. These issues have been resolved.

PCR: 03247 Module: MVR Level: 4

The *Joins* and *Leaves* counters in the SHOW IP MVR COUNTER command output did not count subsequent join or leave requests after the first join or leave. This issue has been resolved.

PCR: 03250 Module: SWI Level: 4

The DELETE SWITCH FILTER command did not work properly when the ENTRY parameter was assigned a range with hyphen (“-”). This issue has been resolved.

PCR: 03252 Module: PIM Level: 3

An assert storm sometimes occurred with PIM-DM. This issue has been resolved.

PCR: 03255 Module: FIREWALL Level: 3

The firewall doubled the IPSPOOF event timeout from 2 minutes to 4 minutes. This issue has been resolved.

PCR: 03256 Module: MLD Level: 3

MLD did not respond correctly when it was in *exclude* mode and it received a request block. This issue has been resolved.

PCR: 03259 Module: SWI Level: 4

On a Rapier 24*i*, when large ping packets were forwarded through a port with ingress limiting, the ping packets were dropped. This issue has been resolved.

PCR: 03261 Module: VLAN, IPG Level: 4

VLAN and IPG packet debugging has been restored.

PCR: 03262 Module: PPP Level: 3

The CREATE CONFIGUATION command adds the PPP TEMPLATE LQR parameter when LQR is enabled. But the configuration script always used "LQR=ON" even when the LQR value was not the default. This meant that if a user entered LQR=40, the configuration would represent LQR=ON. This issue has been resolved.

PCR: 03266 Module: PIM Level: 2

The handling of the upstream neighbour for a *GraftACK* message has been corrected.

PCR: 03269 Module: IPG Level: 4

IGMP reports sometimes contained errors because of MVR. This issue has been resolved.

PCR: 03276 Module: IPG Level: 3

ECMP routing was incorrectly selecting the first route of equal cost found when retrieving routes that were not cached. This issue has been resolved.

PCR: 03277 Module: IPG Level: 3

IGMP Proxy can now forward IGMP Reports.

PCR: 03285 Module: IPG Level: 4

RIP packets can now contain up to 25 routes per packet instead of 24.

PCR: 03288 Module: L2TP Level: 2

When a radius lookup performed by the L2TP Access Concentrator (LAC) failed, the LAC attempted to disconnect the call from its tunnel. If the tunnel had not been created, the device restarted. This issue has been resolved.

PCR: 03291 Module: PPP Level: 2

A PAP authentication failure with PPPoE could cause a fatal error. This issue has been resolved.

PCR: 03292 Module: IP Level: 3

When adding static routes with the ADD IP ROUTE command, the order of the route in the route table was the reverse of the order entered. This issue has been resolved.

PCR: 03293 Module: PPP Level: 3

The MAXSESSION parameter of the SET PPP ACSERVICE command could not be changed when the service was defined over a VLAN. This issue has been resolved.

PCR: 03296 Module: IPG Level: 2

Broadcast TCP packets were being processed by the device, causing fatal errors when firewall SMTP Proxy was configured. Non-unicast TCP packets are now dropped by IP.

PCR: 03298 Module: FIREWALL Level: 3

The SHOW FIREWALL POLICY was not showing the correct debugging items, as set with the ENABLE FIREWALL POLICY DEBUG command. This issue has been resolved.

PCR: 03300 Module: FIREWALL Level: 3

Firewall rules were not being applied to broadcast packets received on a public interface. This issue has been resolved.

PCR: 03302 Module: SWI Level: 3

Following a period of high traffic load, the CPU utilisation would occasionally fail to drop below 40%. This issue has been resolved.

PCR: 03306 Module: IPG Level: 3

IGMP Proxy was setting a delay timer of 1-100 seconds when replying to an IGMP query with a requested maximum delay of 10 seconds. This issue has been resolved.

PCR: 03307 Module: IPG Level: 3

IGMP Proxy did not disable the DR status of an existing IGMP interface when that interface became the IGMP Proxy Upstream. IGMP Proxy also did not enable the DR status of an interface when it became anything other than the IGMP Proxy Upstream. These issues have been resolved.

PCR: 03308 Module: IPG Level: 3

IGMP Proxy now sends an IGMP *Leave* message once all members have left an IGMP group.

PCR: 03317 Module: OSPF Level: 2

Enabling OSPF via the GUI sometimes caused a fatal error. This issue has been resolved.

PCR: 03321 Module: DHCP, Q931, TELNET Level: 4

Debugging for DHCP and Q931 was not being disabled when a Telnet session finished. This issue has been resolved.

PCR: 03332 Module: TTY Level: 2

A log message is now created when a user is forced to logout from an asynchronous port when another user (i.e. someone connected via Telnet) resets the asynchronous connection with the RESET ASYN command.

PCR: 03333 Module: IPG Level: 3

After VRRP was enabled, the link status of the switch ports was shown as UP, even if there was no connection to the ports. This issue has been resolved.

PCR: 03334 Module: MVR Level: 3

The SET IP MVR command now has extra error checking. This is to ensure that if the IMTLEAVE parameter is not specified, the original range of ports set by the CREATE IP MVR command are still contained within the newly specified port range.

PCR: 03336 Module: CORE Level: 4

"AT-A42" was being incorrectly displayed as "AT-A42X-00" in the output of the SHOW SYSTEM command. This issue has been resolved.

PCR: 03341 Module: STP Level: 3

STP ignored some BPDU packets coming in on tagged ports. This issue has been resolved. Now the VLAN tag is ignored on all devices except Rapier *i* Series Switches with multiple STPs on the receiving port.

PCR: 03345 Module: IPG Level: 4

The RESET IP COUNTER=ALL command was not working correctly when issued from the command line. This issue has been resolved.

PCR: 03346 Module: SNMP Level: 4

Sometimes the *Agent Address* field in SNMP traps was not the same as the IP source address. This meant that sometimes the NMS did not send an alarm to the network manager when traps were received from switches. This issue has been resolved.

PCR: 03348 Module: SWI Level: 3

The Uplink card sometimes unnecessarily changed its status from UP to DOWN. This issue has been resolved.

PCR: 03349 Module: BGP Level: 3

When there were a large number of BGP routes, the SHOW BGP ROUTE command sometimes caused an error. This issue has been resolved.

PCR: 03350 Module: IP, SWI Level: 3

A fatal error occurred if an IP ARP route entry was deleted after an IP route filter was added while the IP route was equal to zero. This issue has been resolved.

PCR: 03351 Module: DHCP Level:

Several issues with the DHCP Server have been resolved.

PCR: 03352 Module: PPP Level: 3

The MRU parameter in the SET PPP command was incorrectly handled as an interface parameter when the configuration script was generated. This meant that the OVER parameter was omitted. The MRU parameter is now correctly handled as a link parameter.

PCR: 03353 Module: PPP Level: 3

Dynamic interface details were added through the SET INTERFACE command when the CREATE CONFIGURATION command was executed. This caused errors on startup. This issue has been resolved.

PCR: 03358 Module: SWI Level: 2

Port numbers on a Rapier16f*i* were incorrect. This issue has been resolved. For details on checking the port numbers on a Rapier16 f*i*, see "Checking the Port Map on Rapier16fi Switches" on page 70.

PCR: 03364 Module: PIM Level: 4

PIM will no longer accept obsolete commands.

PCR: 03369 Module: FIREWALL Level: 2

TCP checksums in TCP packets passing through the firewall were being recalculated incorrectly when the TCP setup proxy was disabled, and enhanced NAT was in use. This issue has been resolved.

PCR: 03370 Module: MVR Level: 4

The output of the SHOW IP MVR COUNTER command has been corrected. Also, the output of the SHOW IP MVR command has been modified. The new output is shown in Figure 1:

Figure 1: Example output from the modified SHOW IP MVR command

```
Multicast VLAN
-------------------------------------------------------------------------------
VLAN   Mode         Imtleave   Source Ports   Receiver Ports
                                                 Current Members  Group Address
-------------------------------------------------------------------------------
22     compatible   3          9,10           1-3, 6-7
                                                 1,6              235.1.1.1
                                                 2,7              234.1.1.1
3      compatible   8          12,13          4,5,8,9
                                                 4,8              255.1.1.1
-------------------------------------------------------------------------------
```

PCR: 03372 Module: IPG Level: 3

When a Rapier*i* Series Switch was using layer 3 multicast protocols, IGMP group members on the upstream interface for the multicast stream would always be forwarded to, even if they left the group. This issue has been resolved.

PCR: 03373 Module: HTTP Level: 3

The HTTP proxy server terminated a session when uploading a large file. This issue has been resolved.

PCR: 03375 Module: IPG Level: 2

The following issues with IPv6 have been resolved:

- Incorrect default values were set for the PREFERRED and VALID parameters in the ADD IPV6 PPFEFIX command. The correct default for PREFERRED is 604800 seconds (7 days), and the correct default for VALID is 2592000 seconds (30 days).
- The PREFERRED and VALID parameters in the ADD IPV6 PPFEFIX and SET IPV6 PREFIX commands were accepting values that could make the preferred life time longer than the valid life time.
- The POISONREVERSE parameter in the ADD IPV6 RIP command was not added to the automatic configuration.

PCR: 03379 Module: IPSEC Level: 3

If IPsec was using PPPoE, the initiator continued to keep the IPsec SA even if the PPPoE session failed and the ISAKMP Heartbeat timer expired. This issue has been resolved.

PCR: 03387 Module: PIM, PIM6 Level: 2

A memory leak occurred in IP or IPV6 if PIM-SM received IGMP or MLD reports, and there was no Rendezvous Point for the reported group.

PCR: 03388 Module: DHCP Level: 3

The DHCP lease *Expiry* time showed incorrectly in the SHOW DHCP CLIENT command when the lease straddled across multiple months and years. This issue has been resolved.

PCR: 03393 Module: ISAKMP Level: 3

The allowable UDPPORT range has been changed from 1-5000 to 1-65535 in the ENABLE ISAKMP command.

PCR: 03397 Module: SWI Level: 3

The SHOW SWITCH FDB command output was incorrect when using the Protected VLAN feature. This issue has been resolved.

Features in 86251-03

Patch file details are listed in Table 6:

Table 6: Patch file details for Patch 86251-03.

Base Software Release File	86s-251.rez
Patch Release Date	18-Feb-2003
Compressed Patch File Name	86251-03.paz
Compressed Patch File Size	80884 bytes

Patch 86251-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.5.1, and the following enhancements:

PCR: 02429 Module: IPG Level: 2

When more than two firewall policies were configured, an unexpected switch restart sometimes occurred. This issue has been resolved.

PCR: 03041 Module: PPP Level: 1

PPPoE can now be configured on VLAN interfaces in both Client Mode and Access Concentrator (AC) mode. To configure PPPoE in Client Mode, the physical-interface parameter VLAN*n-servicename* has been added, where *servicename* is 1 to 18 characters in length, and for a PPPoE client is usually supplied by the ISP providing the service. To specify that any service name is acceptable, you can use the special service name ANY.

The modified commands using the *VLANn-servicename* parameter are:

- ADD PPP
- CREATE PPP
- DELETE PPP
- SET PPP
- SHOW PPP

The modified commands and parameters are described at the end of this patch release note in "*PPPoE Client on VLAN Interfaces*" on page 73 For all other unmodified parameters and commands refer to the PPP Chapter in your software reference manual.

PCR: 03050 Module: ETH Level: 3

When an Ethernet port received a MAC Control PAUSE frame it did not stop transmitting packets for a short period of time, as specified in the IEEE 802.3 Ethernet standard. This issue has been resolved.

PCR: 03058 Module: SWI Level: 4

The state of a port not participating in STP was displayed as *disabled*, instead of *broken*. This issue has been resolved.

PCR: 03063 Module: HTTP Level: 1

When HTTP proxy was configured and HTTP requests were sent in quick succession, a fatal error could occur. This issue has been resolved.

PCR: 03065 Module: SWI Level: 2

When the TX cable was unplugged from a fibre port the operating status was incorrectly reported as *UP*. This issue has been resolved.

PCR: 03067 Module: DHCP Level: 1

When replying to a DHCP REQUEST that had passed through a DHCP relay, the broadcast bit of DHCP NAK messages was not being set. This issue has been resolved in accordance with RFC2131.

PCR: 03068 Module: SWI, QOS Level: 2

The SET QOS HWPRIORITY and SET QOS HWQUEUE commands were not accepting all parameters correctly. This meant that the HWPRIORITY and HWQUEUE commands could not be modified with the associated SET command, but had to be made in the configuration script. This issue has been resolved.

PCR: 03069 Module: SWI Level: 1

An issue with Secure Shell clients not being able to connect to a Secure Shell server unless 3DES was installed on both the client and the server has been resolved.

PCR: 03077 Module: CORE Level: 4

The fault LED incorrectly reported a power supply fault (three flashes) on the 48V DC switch versions. This issue has been resolved.

Features in 86251-02

Patch file details are listed in Table 7.

Table 7: Patch file details for Patch 86251-02.

Base Software Release File	86s-251.rez
Patch Release Date	29-January-2003
Compressed Patch File Name	86251-02.paz
Compressed Patch File Size	28756 bytes

PCR: 02542 Module: IPV6 Network affecting: No

The SHOW IPV6 commands were incorrectly including RIPng down routes, and routes on the sending interface. The IPv6 routing table now recognises down routes.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02587 Module: OSPF Network affecting: No

When OSPF was enabled on startup, an OSPF interface would sometimes stay in the DOWN state. This issue has been resolved.

PCR: 03015 Module: SWI Network affecting: No

When ports were added to a trunk group on a Rapier 16, the ports operated in the wrong duplex mode. This issue has been resolved.

PCR: 03029 Module: SWI Network affecting: No

Layer 3 filtering was not correctly modifying a packet's IPDSCP field. This issue has been resolved.

PCR: 03031 Module: FIREWALL Network affecting: No

The ADD FIREWALL POLICY RULE command included an erroneous check on port ranges for non-NAT rules. This check is now restricted to NAT rules.

PCR: 03032 Module: SWI Network affecting: No

If the ENABLE IP IGMP command was executed before the ENABLE SWITCH L3FILTER command, Layer 3 filtering did not discard packets destined for the CPU. This issue has been resolved.

PCR: 03040 Module: IPG Network affecting: No

Sometimes IP flows were not deleted correctly when both directions of the flow were in use. This issue has been resolved.

PCR: 03051 Module: PCI Network affecting: No

The ECPAC card was not working correctly. This issue has been resolved.

Features in 86251-01

Patch file details are listed in Table 8:

Table 8: Patch file details for Patch 86251-01.

Base Software Release File	86s-251.rez
Patch Release Date	23-December-2002
Compressed Patch File Name	86251-01.paz
Compressed Patch File Size	11884 bytes

Patch 86251-01 includes the following enhancements:

PCR: 02331 Module: IPG, ETH Network affecting: No

IP is now informed when an Ethernet interface goes up or down, after a 2.5 second delay.

PCR: 02525 Module: TELNET, PING, IPV6, TCP Network affecting: No

The ADD IPV6 HOST command was not accepting the INTERFACE parameter when adding a host with a link-local address. This issue has been resolved.

PCR: 02527 Module: TCP Network affecting: No

TCP did not send a *TCP Reset* message under some circumstances, for example when the Telnet server was disabled. This issue has been resolved.

PCR: 02552 Module: SWI Network affecting: No

If ingress filtering was supported within trunk groups, ports with ingress filtering enabled were erroneously added to the trunk group. This issue has been resolved.

PCR: 02574 Module: DVMRP Network affecting: No

Some change actions, and the resending of prune messages were not operating correctly. This issue has been resolved.

PCR: 02581 Module: TM Network affecting: No

The test facility was not testing switch ports. This issue has been resolved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.

ICMP Router Discovery Advertisements

Support for Router Discovery

This release supports all of *RFC 1256, ICMP Router Discovery Messages, 1991* as it applies to routers. If this feature is configured, the router sends router advertisements periodically and in response to router solicitations. It does not support the Host Specification section of this RFC.

Benefits

Before an IP host can send an IP packet, it has to know the IP address of a neighbouring router that can forward it to its destination. ICMP Router Discovery messages allow routers to automatically advertise themselves to hosts. Other methods either require someone to manually keep these addresses up to date, or require DHCP to send the router address, or require the hosts to be able to eavesdrop on whatever routing protocol messages are being used on the LAN.

Router Discovery Process

See Table 9 on page 48 for a summary of the processes that occur when Router Discovery advertisements are enabled for interfaces on the router.

Table 9: Router Discovery Process

When ...	Then ...
Router Discovery advertising starts on a router interface because: - the router starts up, or - advertisements are enabled on the switch or on an interface	the router multicasts a router advertisement and continues to multicast them periodically until router advertising is disabled.
a host starts up	the host may send a router solicitation message.
the router receives a router solicitation	the router multicasts an early router advertisement on the multicast interface on which it received the router solicitation.
a host receives a router advertisement	the host stores the IP address and preference level for the advertisement lifetime.
the lifetime of all existing router advertisements on a host expires	the host sends a router solicitation.
a host does not receive a router advertisement after sending a small number of router solicitations	the host waits for the next unsolicited router advertisement
a host needs a default router address	the host uses the IP address of the router or L3 switch with the highest preference level.
Router Discovery advertising is deleted from the physical interface (DELETE IP ADVERTISE command), or the logical interface has ADVERTISE set to NO (SET IP INTERFACE command)	the router multicasts a router advertisement with the IP address(es) that stopped advertising, and a lifetime of zero (0). It continues to periodically multicast router advertisements for other interfaces.
the router receives a router advertisement from another router	the router does nothing but silently discards the message.

Router Advertisement Messages

A *router advertisement* is an ICMP (type 10) message containing:

- In the destination address field of the IP header, the interface's configured advertisement address, either 224.0.0.1 (ALL) or 255.255.255.255 (LIMITED).
- In the lifetime field, the interface's configured advertisement lifetime.
- In the Router Address and Preference Level fields, the addresses and preference levels of all the logical interfaces that are set to advertise.

Router Solicitation Messages

A *router solicitation* is an ICMP (type 10) message containing:

- Source Address: an IP address belonging to the interface from which the message is sent
- Destination Address: the configured Solicitation Address, and
- Time-to-Live: 1 if the Destination Address is an IP multicast address; at least 1 otherwise.

Router Advertisement Interval

The router advertisement *interval* is the time between router advertisements. For the first few advertisements sent from an interface (up to 3), the router sends the router advertisements at intervals of at most 16 seconds. After these initial transmissions, it sends router advertisements at random intervals between the minimum and maximum intervals that the user configures, to reduce the probability of synchronization with the advertisements from other

routers on the same link. By default the minimum is 450 seconds (7.5 minutes), and the maximum is 600 seconds (10 minutes).

Preference Level

The *preference level* is the preference of the advertised address as a default router address relative to other router addresses on the same subnet. By default, all routers and layer 3 switches have the same preference level, zero (0). While it is entered as a decimal in the range `-2147483648..2147483647`, it is encoded in router advertisements as a twos-complement hex integer in the range 0x8000000 to 0x7fffffff. A higher PREFERENCELEVEL is preferred over a lower value.

Lifetime

The *lifetime* of a router advertisement is how long the information in the advertisement is valid. By default, the lifetime of all advertisements is 1800 seconds (30 minutes).

Configuration Procedure

By default, the router does not send router advertisements.

To configure the router to send router advertisements:

1. **Set the physical interface to advertise.**

   For each physical interface that is to send advertisements, add the interface. In most cases the default advertising parameters will work well, but you can change them if required. By default, the router sends router advertisements every 7.5 to 10 minutes, with a lifetime of 30 minutes. These settings are likely to work well in most situations, and will not cause a large amount of extra traffic, even if there are several routers on the LAN. If you change these settings, keep these proportions:

   ```
   LIFETIME=3 x MAXADVERTISEMENTINTERVAL

   MINADVERTISEMENTINTERVAL=0.75 x MAXADVERTISEMENTINTERVAL
   ```

   To change these settings, use one of the commands:

   ```
   ADD IP ADVERTISE INTERFACE=interface
      [ADVERTISEMENTADDRESS={ALL|LIMITED}]
      [MAXADVERTISEMENTINTERVAL=4..1800]
      [MINADVERTISEMENTINTERVAL=3..MAXADVERTISEMENTINTERVAL]
      [LIFETIME=MAXADVERTISEMENTINTERVAL..9000]

   SET IP ADVERTISE INTERFACE=interface
      [ADVERTISEMENTADDRESS={ALL|LIMITED}]
      [MAXADVERTISEMENTINTERVAL=4..1800]
      [MINADVERTISEMENTINTERVAL=3..MAXADVERTISEMENTINTERVAL]
      [LIFETIME=MAXADVERTISEMENTINTERVAL..9000]
   ```

2. **Stop advertising on other logical interfaces.**

   By default, logical interfaces are set to advertise if their physical interface is set to advertise. If the physical interface has more than one logical interface (IP multihoming), and you only want some of them to advertise, set the other logical interfaces not to advertise, using one of the commands:

   ```
   ADD IP INTERFACE=interface IPADDRESS={ipadd|DHCP}
      ADVERTISE=NO [other-ip-parameters]

   SET IP INTERFACE=interface ADVERTISE=NO [other-ip-
      parameters]
   ```

3. **Set preference levels.**

   By default, every logical interface has the same preference for becoming a default router (mid range, 0). To give a logical interface a higher preference, increase the PREFERENCELEVEL. To give it a lower preference, decrease

this value. If it should never be used as a default router, set it to NOTDEFAULT.

```
ADD IP INTERFACE=interface IPADDRESS={ipadd|DHCP}
    PREFERENCELEVEL={-2147483648..2147483647|NOTDEFAULT}
    [other-ip-parameters]

SET IP INTERFACE=interface
    [PREFERENCELEVEL={-2147483648..2147483647|NOTDEFAULT}]
    [other-ip-parameters]
```

4. Enable advertising.

Enable router advertisements on all configured advertising interfaces, using the command:

```
ENABLE IP ADVERTISE
```

5. Check advertise settings.

To check the router advertisement settings, use the command:

```
SHOW IP ADVERTISE
```

Commands These commands have been modified:

- ADD IP INTERFACE
- SET IP INTERFACE

These commands are new:

- ENABLE IP ADVERTISE
- ADD IP ADVERTISE
- SET IP ADVERTISE
- SHOW IP ADVERTISE

Two new parameters have been added to the ADD IP INTERFACE and SET IP INTERFACE commands:

```
ADD IP INTERFACE=interface IPADDRESS={ipadd|DHCP}
    [ADVERTISE={YES|NO}]
    [PREFERENCELEVEL={-2147483648..2147483647|NOTDEFAULT}]
    [other-ip-parameters]

SET IP INTERFACE=interface [ADVERTISE={YES|NO}]
    [PREFERENCELEVEL={-2147483648..2147483647|NOTDEFAULT}]
    [other-ip-parameters]
```

where:

- *interface* is an interface name formed by concatenating a Layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number in the range 0 to 15. If a logical interface is not specified, 0 is assumed.

The ADVERTISE parameter specifies whether or not the logical interface is to send Router Discovery advertisements. The default is YES.

The PREFERENCELEVEL parameter specifies the preference of the address as a default router address relative to other router addresses on the same subnet, as a decimal integer. If the minimum value -2147483648 or the keyword NOTDEFAULT is specified, the address is not to be used by neighbouring hosts as a default address, even though it may be advertised. The default value is the mid range 0.

ENABLE IP ADVERTISE

Syntax `ENABLE IP ADVERTISE`

Description This command globally enables ICMP Router Discovery advertisements on the router. However the device will not send or process Router Discover messages until at least one IP interface is configured using the ADD IP ADVERTISE INTERFACE command.

Examples To enable Router Discovery advertisements, use the command:

```
ENABLE IP ADVERTISE
```

See Also ADD IP ADVERTISE INTERFACE
ADD IP INTERFACE
DISABLE IP ADVERTISE
SET IP ADVERTISE INTERFACE
SET IP INTERFACE
SHOW IP ADVERTISE

DISABLE IP ADVERTISE

Syntax `DISABLE IP ADVERTISE`

Description This command globally disables ICMP Router Discovery advertisements on the device. All transmitting and processing of Router Discovery messages ceases immediately on all interfaces.

Examples To disable Router Discovery advertisements, use the command:

```
DISABLE IP ADVERTISE
```

See Also DELETE IP ADVERTISE INTERFACE
ENABLE IP ADVERTISE
SET IP ADVERTISE INTERFACE
SHOW IP ADVERTISE

ADD IP ADVERTISE INTERFACE

Syntax

```
ADD IP ADVERTISE INTERFACE=interface
   [ADVERTISEMENTADDRESS={ALL|LIMITED}]
   [MAXADVERTISEMENTINTERVAL=4..1800]
   [MINADVERTISEMENTINTERVAL=3..MAXADVERTISEMENTINTERVAL]
   [LIFETIME=MAXADVERTISEMENTINTERVAL..9000]
```

where:

- *interface* is an interface name formed by concatenating an interface type and an interface instance (e.g. vlan1).

Description This command adds ICMP Router Discovery advertising to a single physical IP interface. The interface will only send router advertisements if it has been globally enabled with the ENABLE IP ADVERTISE command.

The ADVERTISEMENTADDRESS parameter specifies the IP destination address to be used for multicast advertisements sent from the interface. If ALL is specified, the destination is the All-systems multicast address, 224.0.0.1. If LIMITED is specified, the destination is the limited-broadcast address, 255.255.255.255. The default is ALL.

The MAXADVERTISEMENTINTERVAL parameter specifies the maximum time in seconds between sending multicast advertisements from the interface. The default is 600 seconds.

The MINADVERTISEMENTINTERVAL parameter specifies the minimum time in seconds between sending multicast advertisements from the interface. The default value is 450 seconds.

The LIFETIME parameter specifies the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts. The default value is 1800 seconds.

If you change the advertising intervals, keep these proportions:
LIFETIME=3 x MAXADVERTISEMENTINTERVAL
MINADVERTISEMENTINTERVAL=0.75 x MAXADVERTISEMENTINTERVAL

Examples To add Router Discovery advertising to VLAN2, modify the default ADVERTISEMENTADDRESS to the limited-broadcast address 255.255.255.255 and modify the MAXADVERTISEMENTINTERVAL to 1000 seconds, use the command:

```
ADD IP ADVERTISE INTERFACE=VLAN2 ADVERTISEMENTADDRESS=LIMITED
   MAXADVERTISEMENTINTERVAL=1000
   MINADVERTISEMENTINTERVAL=750 LIFETIME=3000
```

See Also ENABLE IP ADVERTISE
DISABLE IP ADVERTISE
DELETE IP ADVERTISE INTERFACE
SET IP ADVERTISE INTERFACE
SET IP INTERFACE
ADD IP INTERFACE

DELETE IP ADVERTISE INTERFACE

Syntax `DELETE IP ADVERTISE INTERFACE=`*`interface`*

where:

- *interface* is an interface name formed by concatenating an interface type and an interface instance (e.g. eth0 vlan1).

Description This command deletes ICMP Router Discovery advertising from a single physical IP interface and its configuration from a physical IP interface.

Example To delete Router Discovery from vlan1, use the command:

```
DELETE IP ADVERTISE INTERFACE=vlan1
```

See Also DISABLE IP ADVERTISE
ENABLE IP ADVERTISE
ADD IP DISCOVERY INTERFACE
SET IP DISCOVERY INTERFACE

SET IP ADVERTISE INTERFACE

Syntax

```
SET IP ADVERTISE INTERFACE=interface
   [ADVERTISEMENTADDRESS=ALL|LIMITED]
   [MAXADVERTISEMENTINTERVAL=4..1800]
   [MINADVERTISEMENTINTERVAL=3..MAXADVERTISEMENTINTERVAL]
   [LIFETIME=MAXADVERTISEMENTINTERVAL..9000]
```

where:

- *interface* is an interface name formed by concatenating an interface type and an interface instance (e.g. vlan1).

Description This command modifies the Router Discovery advertisement settings on a single IP interface.

The ADVERTISEMENTADDRESS parameter specifies the IP destination address to be used for multicast advertisements sent from the interface. If ALL is specified, the destination is the All-systems multicast address, 224.0.0.1. If LIMITED is specified, the destination is the limited-broadcast address, 255.255.255.255. The default is ALL.

The MAXADVERTISEMENTINTERVAL parameter specifies the maximum time in seconds allowed between sending multicast advertisements from the interface. The default value is 600 seconds.

The MINADVERTISEMENTINTERVAL parameter specifies the minimum time in seconds allowed between sending multicast advertisements from the interface. The default value is 450 seconds.

The LIFETIME parameter specifies the maximum length of time that the advertised addresses are to be considered as valid router addresses by hosts. The default value is 1800 seconds.

If you change the advertising intervals, keep these proportions:
LIFETIME=3 x MAXADVERTISEMENTINTERVAL
MINADVERTISEMENTINTERVAL=0.75 x MAXADVERTISEMENTINTERVAL

Examples To modify the ADVERTISEMENTADDRESS to the limited-broadcast address 255.255.255.255 and set the MAXADVERTISEMENTINTERVAL to 1000 seconds on VLAN3:

```
SET IP ADVERTISE INTERFACE=VLAN3 ADVERTISEMENTADDRESS=LIMITED
   MAXADVERTISEMENTINTERVAL=1000
   MINADVERTISEMENTINTERVAL=750 LIFETIME=3000
```

See Also DISABLE IP DISCOVERY
DELETE IP DISCOVERY INTERFACE
ENABLE IP DISCOVERY
ADD IP DISCOVERY INTERFACE

SHOW IP ADVERTISE

Syntax `SHOW IP ADVERTISE`

Description This command displays the Router Discovery advertising configuration for all IP interfaces.

Figure 2: Example output from the SHOW IP ADVERTISE command.

```
Router Advertisement ............... Enabled

Interface ........................... vlan2
    Advertisement Address ........... 224.0.0.1 (all)
    Max Advertisement Interval ...... 600
    Min Advertisement Interval ...... 450
    Lifetime ........................ 1800
    Advertisements sent ............. 1
    Solicitations received .......... 0

    Logical Interface   IP Address      Advertise   Preference Level
    ---------------------------------------------------------------
    vlan2-0             192.168.1.1     Yes        -1
    vlan2-1             192.168.2.1     Yes         1
```

Table 10: Parameters displayed in the output of the SHOW IP ADVERTISE command.

Parameter	Meaning
Router Advertisement	Whether the ICMP Router Discovery advertisements feature is enabled or disabled on the router.
Interface	The IP physical interface.
Advertisement Address	Either the All-systems multicast address (224.0.0.1) or the Limited-broadcast address (255.255.255.255).
Max Advertisement Interval	The maximum time allowed between sending multicast router advertisements.
Min Advertisement Interval	The minimum time allowed between sending multicast router advertisements.
Lifetime	The maximum time that the advertised address should be treated as valid.
Advertisements sent	How many router advertisements the interface has sent since advertising was enabled.
Solicitations received	How many router solicitations the interface has received since advertising was enabled.
Logical Interface	An IP logical interface on this physical interface.

Table 10: Parameters displayed in the output of the SHOW IP ADVERTISE command. (Continued)

Parameter	Meaning
IP Address	An IP address assigned to the interface.
Advertise	Whether the address for this logical interface should be advertised.
Preference Level	The preferability of the address as a default router address relative to other router addresses on the same subnet.

See Also

DISABLE IP DISCOVERY
DELETE IP DISCOVERY INTERFACE
ENABLE IP DISCOVERY
ADD IP DISCOVERY INTERFACE
SET IP DISCOVERY INTERFACE

Old Router Discover Process

Before an IP host can send IP packets, it needs the IP address of a router that can forward it to its destination. When router advertisements are enabled, the router multicasts router advertisements periodically on any interfaces that are configured to advertise. When hosts receive these messages, they store them for the specified lifetime. They forward traffic to the IP address of the router with the highest preference level specified in the router advertisement.

When a host first starts up, it may send one, or a small number of router solicitations to prompt a quicker router advertisement, instead of waiting for the next router advertisement to arrive automatically. When the router receives a router solicitation with an IP address, it immediately multicasts an early router advertisement.

For the first few advertisements sent from an interface (up to 3), if the randomly chosen interval is greater than 16 seconds, the router sends the router advertisements at intervals of at most 16 seconds. After these initial transmissions, it sends router advertisements at random intervals between the minimum and maximum intervals that the user configures, to reduce the probability of synchronization with the advertisements from other routers on the same link.

If either an interface, or router advertisements on an interface are disabled, the router sends a final multicast advertisement on the interface with a lifetime field of zero. If some of the IP addresses have advertising disabled, while others continue to advertise, the router sends a router advertisement containing the remaining IP addresses.

The router does not behave as a Router Discovery host to discover other routers on the LAN; it discards any router advertisements that it receives from other routers.

Adopting the VRRP IP Address

Benefits

The VRRP master router can *adopt* the IP address of the virtual router (VR), and respond to the following packets destined for the VR IP address, even if it does not own this IP address on any of its interfaces:

- ICMP echo requests (pings)
- Telnet and SSH connection requests
- HTTP and SSL GUI management requests
- SNMP requests, and
- DNS relay requests

VRRP IP Address Adoption allows continuous accessibility of the VR IP address even as the VR master changes. Using this feature:

- You can easily tell whether the VR is functioning, by pinging the single VR IP address.
- You can easily monitor the performance of the VR, regardless of which participating router is acting as master.
- DNS relay can continue functioning via the same IP address at all times.

Risks

When VR IP Address Adoption is used, the master router accepts packets destined for the virtual router, even though it may not own this IP address. This does not conform to RFC 2338. Because the same IP address refers to different devices at different times, there is a risk of confusion arising. This risk can be reduced by a suitable network management policy.

Recommendations

Before using VR IP address adoption, consider the following guidelines to avoid confusion:

- Ensure that the VR has an IP address that is different from the interface IP addresses of any of the individual routers in the VR.
- Ensure that all routers in the virtual router use VRRP IP Address Adoption (or that none do).
- Use the VR IP address to monitor the VR master. Be aware that this does not give information about one particular participating router, but about the current VR master, whichever participating router is acting as the master at the time.
- When changing the configuration of the participating routers using Telnet, GUI or SNMP, configure each device individually by pointing to their individual IP addresses.
- When changing the configuration of the participating routers, do not use the VR IP address. Only one device, the VR master, is responding to this IP address, and you may not know which device it is.

Configuration

To configure VR IP Address Adoption, use the new parameter, ADOPTVRIP, that has been added to the CREATE VRRP and SET VRRP commands:

```
CREATE VRRP=vr-identifier OVER=physical-interface
   IPADDRESS=ipadd [ADOPTVRIP={ON|OFF}] [other-vrrp-
   parameters]

SET VRRP=vr-identifier [ADOPTVRIP={ON|OFF}] [other-vrrp-
   parameters]
```

The ADOPTVRIP parameter specifies that when the switch is acting as the VRRP master it should respond to requests directed at any IP address that it is backing up, even if it does not own that address. If it does not own the address the access requests that the switch will permit are limited to: ICMP echo requests (pings), Telnet, SSH, HTTP and SSL GUI, SNMP and DNS relay. All other types of access to the address will be ignored. The default is OFF.

If you set ADOPTVRIP to ON, give the VR an IP address that is different from the interface IP addresses of any of the individual routers in the VR, and only use the VR IP address to monitor the VR, not to configure any of its participating routers. Otherwise you risk confusion when you monitor or configure individual routers. See "ICMP Router Discovery Advertisements" on page 47 for more about risks and recommendations.

Configure all the switches in a virtual router with the same values for the VRRP virtual router identifier, IP address, adopt VR IP address mode, advertisement interval, preempt mode, authentication type and password. Inconsistent configuration will cause advertisement packets to be rejected and the virtual router will not perform properly.

To display the value of the new parameter, use the SHOW VRRP command.

Table 11: New parameter displayed in the output of the SHOW VRRP command

Parameter	Meaning
Adopt VR IP Address(es)	Whether or not the switch should respond to ICMP echo, Telnet, GUI, SNMP and DNS relay service requests targeted at the VR IP address(es) associated with the virtual router, even if it does not own those address(es).

MLD Snooping

Multicast Listener Discovery (MLD) snooping enables the switch to forward IPv6 multicast traffic intelligently, instead of flooding it out all ports in the VLAN. With MLD snooping, the switch passively listens to MLD joins/reports and leaves/done messages, to identify the switch ports that have received joins and/or leaves from devices attached to them. Multicast traffic will only be forwarded to those ports. MLD snooping will also identify ports that are connected to another router or switch and forward messages out those ports appropriately.

MLD snooping is performed at Layer 2 on VLAN interfaces automatically. By default, the switch will only forward traffic out those ports with routers or IPv6 multicast listeners, therefore it will not act as a simple hub and flood all IPv6 multicast traffic out all ports. MLD snooping is independent of the MLD and Layer 3 configuration, so an IPv6 interface does not have to be attached to the VLAN, and MLD does not have to be enabled or configured.

MLD snooping is enabled by default. To disable it, use the command:

```
DISABLE MLDSNOOPING
```

Note that IPv6 multicast packets will flood the VLAN when MLD snooping is disabled.

To enable MLD snooping, use the command:

```
ENABLE MLDSNOOPING
```

To display debugging information, use the command:

```
ENABLE MLDSNOOPING DEBUG
```

This command displays the ports that are currently receiving MLD packets and the ports that are being added or taken off the switch's multicast group membership registration.

To disable debugging, use the command:

```
DISABLE MLDSNOOPING DEBUG
```

To display information about MLD snooping, use the command:

```
SHOW MLDSNOOPING COUNTER
```

For more information, including limitations on which addresses and packet types can be snooped, see the *IPv6 Multicasting* chapter of the *Software Reference*.

Ping Polling of Device Reachability

This enhancement enables the router or switch to regularly check whether or not it can reach a device. It also enables a trigger to activate on the router or switch when the device becomes unreachable. While the device is unreachable, the router or switch continues to monitor the device's reachability, and another trigger can be set to activate when the device becomes available again. For example, the first trigger's script could open and configure an alternative link if the device at the other end of a preferred link became unavailable. The second trigger's script would automatically return traffic to the preferred link as soon as it was available again.

To determine the device's reachability, the router or switch will regularly send ICMP Echo Request packets ("pings") to the device. As long as the router or switch receives ping responses from the device, it considers the device to be reachable. After the router or switch has not received a reply to a set number of ICMP Echo Requests, it considers the device to be unreachable. It continues to try to ping the device, at an increased rate. After it receives a set number of responses, it considers the device to be reachable again.

Configuring the router or switch to determine a device's reachability and respond to changes in reachability involves the following steps:

- Create a polling instance, to periodically ping the device
- Create scripts to run when the device becomes unreachable and when it becomes reachable again
- Configure triggers to run these scripts.

To create a polling instance, use the command:

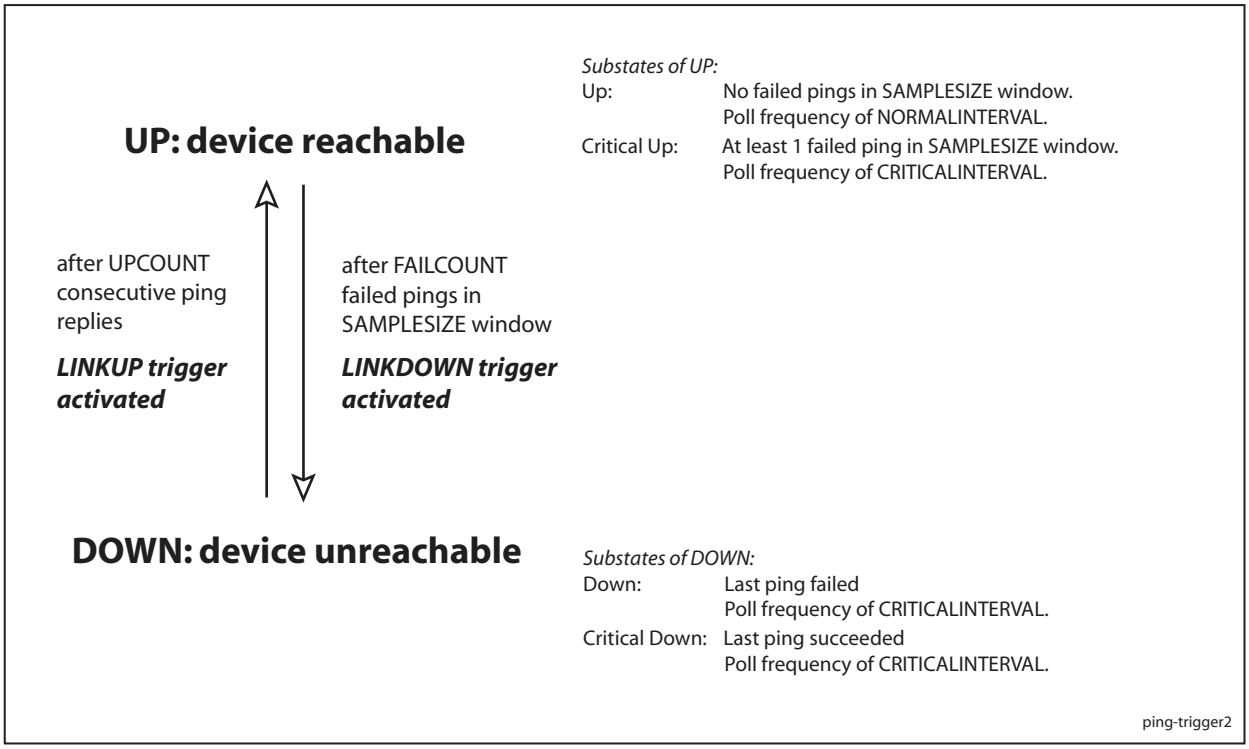
```
ADD PING POLL=poll-id IPADDRESS={ipadd|ipv6add[%interface]}
    [CRITICALINTERVAL=1..65535]
    [DESCRIPTION=poll-description] [FAILCOUNT=1..100]
    [LENGTH=4..1500] [NORMALINTERVAL=1..65535]
    [SAMPLESIZE=1..100] [SIPADDRESS={ipadd|ipv6add}]
    [TIMEOUT=1..30] [UPCOUNT=1..100]
```

- where *poll-id* is a number from 1 to 100, and identifies the polling instance in the trigger commands and in other PING POLL commands. The router or switch can poll up to 100 IP addresses at once.

The NORMALINTERVAL parameter specifies the time period between pings when the device is reachable. By default, this is set to 30 seconds. The CRITICALINTERVAL parameter specifies the time period between pings when the router or switch has not received a reply to at least one ping and when the device is unreachable. The default is 1 second. The CRITICALINTERVAL enables the router or switch to quickly observe changes in the state of the device, and should be set to a much lower value than the NORMALINTERVAL.

The number of pings that the router or switch will examine to consider a change in state is controlled by three parameters: FAILCOUNT, SAMPLESIZE, and UPCOUNT. The FAILCOUNT is the number of pings that must be unanswered for the router or switch to consider the device unreachable. The default is 5. The SAMPLESIZE is the total number of pings within which the FAILCOUNT number of pings must be unanswered. If SAMPLESIZE and FAILCOUNT are the same, the unanswered pings must be consecutive. If SAMPLESIZE is greater than FAILCOUNT, a device that does not always reply to pings may be declared unreachable. By default, SAMPLESIZE is equal to FAILCOUNT. The UPCOUNT is the number of consecutive pings that must be answered for the router or switch to consider the device reachable again. The default is 30. The interaction between these parameters is shown in Figure 3.

Figure 3: The interaction between states and parameters for ping polling.



After you have configured the ping polling instance, specify a script or scripts to run when the device becomes unreachable, using the command:

```
CREATE TRIGGER=trigger-id MODULE=PING EVENT=DEVICEDOWN
   POLL=poll-id SCRIPT=filename... [other-options...]
```

Then specify a script or scripts to run when the device becomes reachable again, using the command:

```
CREATE TRIGGER=trigger-id MODULE=PING EVENT=DEVICEUP
   POLL=poll-id SCRIPT=filename... [other-options...]
```

where *filename* is the name of the script file, and will have a `.scp` extension.

Finally, enable the polling instance, using the command:

```
ENABLE PING POLL=poll-id
```

Ping polling is only available for IP and IPv6 (ICMP and ICMP6 Echo Request and Reply packets), not for IPX, AppleTalk or OSI.

Enable and Disable ICMP Messages

The *Internet Control Message Protocol* (ICMP) allows routers to send error and control messages to other routers or hosts. It provides the communication between IP software on one system and IP software on another.

This enhancement allows the switch to enable or disable some ICMP messages when directed by the network manager.

The ICMP messages that are able to be enabled or disabled are:

- Network unreachable (RFC792 Type 3 Code 0)
- Host unreachable (RFC792 Type 3 Code 1)
- ICMP redirect messages (RFC792 Type 5 Code 0, 1, 2, 3)

Network Unreachable

This message indicates that the switch does not know how to reach the destination network.

Host Unreachable

This message indicates that the switch does not know how to reach the host.

ICMP Redirect

This message is sent to a local host to tell it that its target is located on the same LAN (no routing is required) or when it detects a host using a non-optimal route (usually because a link has failed or changed its status) on a directly connected router to advise of a better route to a particular destination.

For more information on ICMP, see the IP Chapter in your switch's Software Reference manual.

Commands

This enhancement introduces three new commands:

- DISABLE IP ICMPREPLY
- ENABLE IP ICMPREPLY
- SHOW IP ICMPREPLY

DISABLE IP ICMPREPLY

Syntax

```
DISABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]
```

Description This command disables ICMP reply messages.

If ALL is specified, all configurable ICMP message replies are disabled. If NETUNREACH is specified, all network unreachable message replies are disabled (RFC792 Type 3 Code 0). If HOSTUNREACH is specified, all host unreachable message replies are disabled (RFC792 Type 3 Code 1). If REDIRECT is specified, all ICMP redirect message replies are disabled (RFC792 Type 5 Code 0, 1, 2, 3).

Example To disable all configurable ICMP messages, use the command:

```
DISABLE IP ICMPREPLY=ALL
```

See Also ENABLE IP ICMPREPLY
DISABLE IP ECHOREPLY
SHOW IP ICMPREPLY

ENABLE IP ICMPREPLY

Syntax

```
ENABLE IP
   ICMPREPLY[={ALL|NETUNREACH|HOSTUNREACH|REDIRECT}]
```

Description This command enables ICMP reply messages.

If ALL is specified, all configurable ICMP message replies are enabled. If NETUNREACH is specified, all network unreachable message replies are enabled (RFC792 Type 3 Code 0). If HOSTUNREACH is specified, all host unreachable message replies are enabled (RFC792 Type 3 Code 1). If REDIRECT is specified, all ICMP redirect message replies are enabled (RFC792 Type 5 Code 0, 1, 2, 3).

Example To enable all configurable ICMP messages, use the command:

```
ENABLE IP ICMPREPLY=ALL
```

See Also ENABLE IP ECHOREPLY
DISABLE IP ICMPREPLY
SHOW IP ICMPREPLY

SHOW IP ICMPREPLY

Syntax `SHOW IP ICMPREPLY`

Description This command display the status of configurable ICMP messages (Figure

Figure 4: Example output from the SHOW IP ICMPREPLY command:

```
SHOW IP ICMP REPLY MESSAGES
--------------------------------------------------------------------------------
ICMP REPLY MESSAGES:
  Network Unreachable ............... disabled
  Host Unreachable .................. disabled
  Redirect .......................... enabled
--------------------------------------------------------------------------------
```

Table 5: Parameters in the output of the SHOW IP ICMPREPLY command.

Parameter	Meaning
ICMP Reply Messages	A list of ICMP configurable reply messages and whether they are enabled or disabled.

Static IGMP

This section describes an enhancement to the *Internet Group Management Protocol* (IGMP), which is supplied as a patch on Software Releases 2.5.1 for Rapier *i* Series switches.

It is possible to have a network segment that either has no multicast group members, or has a host that is unable to report its group membership with IGMP. In such cases, no multicast traffic is sent to the network segment. This enhancement provides a mechanism for the user to pull down multicast traffic to the segment.

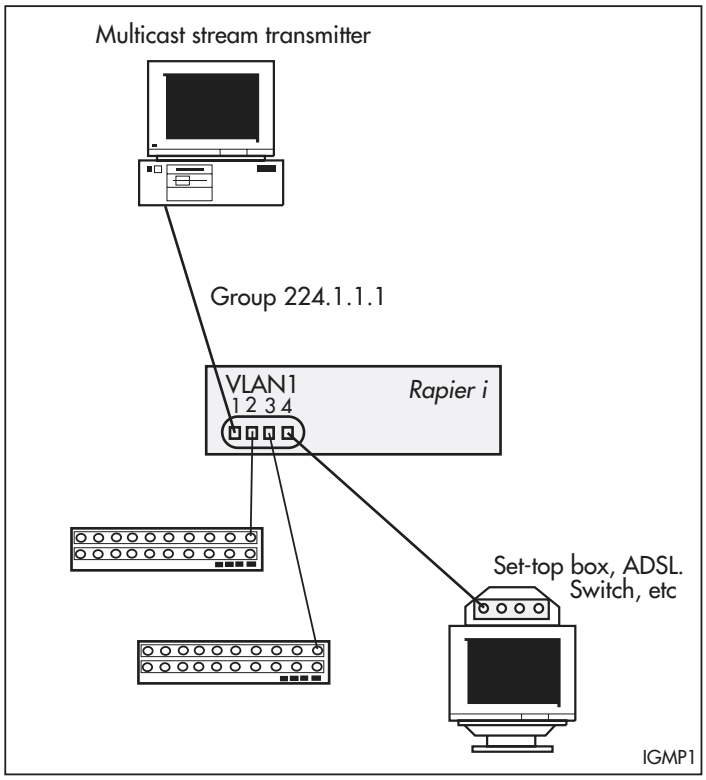
Currently the switch forwards multicast data on a dynamic basis to hosts who have joined the multicast group. This enhancement allows the user to instruct the switch to forward multicast data over a specified interface and port, as shown in Figure 6 on page 63. This capability is essential for sending multicast traffic to hosts that cannot report their group membership with IGMP. It plays an important role in video over ADSL applications.

Figure 6 on page 63 illustrates a switch forwarding the multicast stream to a set-top box after a user specifies that group 224.1.1.1 multicast data should be forwarded out of port 4 of VLAN1.

Unlike conventional IGMP membership, this user-specified static membership never times out.

The user will also be able to filter some IGMP debug messages by source IP address and group destination address.

Figure 6: Forwarding multicast data over a specified interface and port.



Configuration Example

The following configuration example illustrates the steps required to create a static IGMP association. It assumes that *vlan1* has already been configured as an IP interface on the switch.

6. Enable IGMP on the switch.

```
ENABLE IP IGMP
```

7. Enable IGMP on vlan1.

This must be done before the static IGMP association is created.

```
ENABLE IP IGMP INTERFACE=VLAN1
```

8. Create the static IGMP association.

The multicast data for the group specified by the DESTINATION parameter will be forwarded over the ports specified by the PORT parameter. If the PORT parameter is not entered, the association will default to all ports belonging to the interface.

```
CREATE IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1
   PORT=1-4
```

9. Check the configuration.

Check that the static IGMP association has been created and IGMP is enabled.

```
SHOW IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1
```

Commands

This enhancement modifies one command:

- SHOW IP IGMP
  This command now includes a DESTINATION parameter. Only the modified parts of the command text are shown below.

and has seven new commands:

- ADD IP IGMP DESTINATION
- CREATE IP IGMP DESTINATION
- DELETE IP IGMP DESTINATION
- DESTROY IP IGMP DESTINATION
- DISABLE IP IGMP DEBUG
- ENABLE IP IGMP DEBUG
- SHOW IP IGMP DEBUG

Modified Command

SHOW IP IGMP

Syntax

```
SHOW IP IGMP [COUNTER] [INTERFACE=interface]
    [DESTINATION=ipaddress]
```

where:

- *ipaddress* is an existing IGMP group destination address, or a pattern matching one or more IGMP group destination addresses.

Description

The enhancement to this command is the addition of a new parameter, DESTINATION.

The DESTINATION parameter allows the user to screen out all IGMP information not related to the specified group destination address, i.e. only information relating to the multicast group destination address is displayed. Any of the four octets of the IP address may be replaced by '*' to enable wildcard matches, e.g. 224.*.*.*.

If both the COUNTER and DESTINATION parameters are specified, counters will only be displayed for the interfaces that have a group destination address matching that of the DESTINATION parameter.

Static groups will have their refresh time displayed as "Infinity".

All other parameters for this command remain the same. See the IP chapter in your switch's software reference for more information.

Examples

To display information about all group destination addresses starting with "224" on *vlan1*, use the command:

```
SHOW IP IGMP INTERFACE=VLAN1 DESTINATION=224.*.*.*
```

Figure 7: Example output from the SHOW IP IGMP DESTINATION command showing Static Groups.

```
IGMP Protocol
-------------------------------------------------------------------------------
Status ........................... Enabled
Default Query Interval ........... 125 secs
Default Timeout Interval ......... 270 secs

Last Member Query Interval ....... 10 (1/10secs)
Last Member Query Count .......... 2
Robustness Variable .............. 2
Query Response Interval .......... 100 (1/10secs)

Interface Name .......... vlan1               (DR)
IGMP Proxy .............. Off
Group List ..............

  Group. 224.0.1.22         Static association          Refresh time Infinity
  Ports  1,3
  Static Ports 3
```

Table 1: Parameters in the output of the SHOW IP IGMP DESTINATION command.

Parameter	Meaning
Static Ports	A list of the static ports; a subset of the ports listed in the Ports field. The Static Ports field is only displayed for static groups on a VLAN.

See Also SHOW IP IGMP DEBUG

New Commands

ADD IP IGMP DESTINATION

Syntax

```
ADD IP IGMP DESTINATION=ipaddress INTERFACE=interface
   PORT={ALL|port-list}
```

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded. This must be a VLAN interface.
- *port-list* is a port number, a range of port numbers (specified as a-b), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port, including uplink ports.

Description

This command adds additional ports, through which multicast data is forwarded.

The DESTINATION parameter specifies the IP address from where multicast data is forwarded.

The INTERFACE parameter specifies the interface over which multicast data is forwarded. This must be a VLAN interface, e.g. VLAN1.

The static IGMP association identified by the DESTINATION and INTERFACE parameters must already exist.

The PORT parameter specifies the ports through which multicast data is forwarded. If any of the ports specified in the port list are already part of the association, or are not valid ports for the specified interface, an error message is displayed.

A port may belong to several associations if it belongs to several interfaces (i.e. if there are overlapping VLANs). If one of the ports specified in the port list already has a dynamic IGMP host, it will be replaced by the new static entry. If ALL is specified, all ports belonging to that interface will forward multicast data.

Examples

To add port 5 to the list of ports through which multicast data for 224.1.2.3 will be forwarded over *vlan1*, use the command:

```
ADD IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1 PORT=5
```

See Also

DELETE IP IGMP DESTINATION
SHOW IP IGMP

CREATE IP IGMP DESTINATION

Syntax

```
CREATE IP IGMP DESTINATION=ipaddress INTERFACE=interface
   [PORT={ALL|port-list}]
```

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded.
- *port-list* is a port number, a range of port numbers (specified as a-b), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port, including uplink ports.

Description

This command creates a static multicast association to forward multicast data from a multicast group to one or more ports.

The DESTINATION parameter specifies the IP address from where multicast data is forwarded.

The INTERFACE parameter specifies the interface over which multicast data is forwarded.

The static IGMP association identified by the DESTINATION and INTERFACE parameters must not already exist.

The PORT parameter specifies the ports through which multicast data is forwarded. If any of the ports specified in the port list are not valid ports for the specified interface, an error message is displayed. An empty port list can be specified by giving no value to the PORT parameter. Ports may be added later using the ADD IP IGMP DESTINATION command. If ALL is specified, or if the PORT parameter is not entered, all ports belonging to that interface will forward multicast data.

Since static IGMP associations are identified by the combination of destination and interface, one destination or interface may belong to several different associations. Also, ports may belong to several associations if there are overlapping VLANs. There is no conflict with existing standard (dynamic) IGMP hosts: if a new static association's port already has a dynamic IGMP host, the new static entry will replace it.

IGMP destinations added with this command will never time out. They are removed with the DESTROY IP IGMP DESTINATION command.

Examples

To forward multicast data to 224.1.2.3 out ports 1 to 4 using *vlan1*, use the command:

```
CREATE IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1 PORT=1-4
```

See Also

ADD IP IGMP DESTINATION
DESTROY IP IGMP DESTINATION

DELETE IP IGMP DESTINATION

Syntax `DELETE IP IGMP DESTINATION=`*`ipaddress`* `INTERFACE=`*`interface`*
`PORT={ALL|`*`port-list`*`}`

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded. This must be a VLAN interface.
- *port-list* is a port number, a range of port numbers (specified as a-b), or a comma separated list of port numbers and/or ranges. Port numbers start at 1 and end at m, where m is the highest numbered Ethernet port, including uplink ports.

Description This command deletes ports from a static multicast group. Multicast data from the multicast group will no longer be forwarded out the port(s). The static association identified by the DESTINATION and INTERFACE parameters must exist for this command to succeed.

If any of the ports specified in the port list are not assigned to this static association, an error message is displayed. When the last port is removed, the static association will still exist, although it will have no functionality until ports are added again. To destroy the entire static association, use the DESTROY IP IGMP DESTINATION command.

Examples To remove ports 1-4 from the list of ports through which multicast data for 224.1.2.3 will be forwarded over *vlan1*, use the command:

```
DELETE IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1 PORT=1-4
```

See Also CREATE IP IGMP DESTINATION
SHOW IP IGMP

DESTROY IP IGMP DESTINATION

Syntax `DESTROY IP IGMP DESTINATION=`*`ipaddress`* `INTERFACE=`*`interface`*

where:

- *ipaddress* is an existing IGMP group destination address.
- *interface* is the name of the interface over which multicast data is forwarded.

Description This command destroys a static IGMP association. It is not necessary to delete the ports first. The static IGMP association identified by the DESTINATION and INTERFACE parameters must already exist for this command to succeed.

Examples To stop the switch forwarding all multicast data for 224.1.2.3 over *vlan1*, use the command:

```
DESTROY IP IGMP DESTINATION=224.1.2.3 INTERFACE=VLAN1
```

See Also CREATE IP IGMP DESTINATION

DISABLE IP IGMP DEBUG

Syntax `DISABLE IP IGMP DEBUG`

Description This command disables all IGMP debugging messages and resets the DESTINATION and SOURCEIPADDRESS parameters set in the ENABLE IP IGMP DEBUG command to ALL. Debugging is disabled by default.

Examples To disable all IGMP debugging messages and reset the IGMP debug message filters to ALL, use the command:

```
DISABLE IP IGMP DEBUG
```

See Also SHOW IP IGMP DEBUG

ENABLE IP IGMP DEBUG

Syntax

```
ENABLE IP IGMP DEBUG [DESTINATION={ALL|ipaddress}]
   [SOURCEIPADDRESS={ALL|ipaddress2}]
```

where:

- *ipaddress* is an IGMP group destination address.
- *ipaddress2* is the IP address of a host that responds to IGMP queries.

Description This command enables IGMP debugging of destination and source IP addresses. Debugging is disabled by default.

The DESTINATION parameter specifies the destination multicast group address for debugging. The default is ALL.

The SOURCEIPADDRESS specifies the host IP address responding to IGMP queries. The default is ALL.

If DESTINATION and SOURCEIPADDRESS are both specified, only debug messages that match both parameters are displayed. Some debug messages are displayed before the packet is fully decoded, and are unable to be filtered.

Examples To enable debugging information relating to IGMP host 10.41.0.22, use the command:

```
ENABLE IP IGMP DEBUG SOURCEIPADDRESS=10.41.0.22
```

To show all IGMP debug messages, use the command:

```
ENABLE IP IGMP DEBUG
```

See Also SHOW IP IGMP DEBUG

SHOW IP IGMP DEBUG

Syntax `SHOW IP IGMP DEBUG`

Description This command shows the IGMP debugging options that have been set.

Figure 8: Example output from SHOW IP IGMP DEBUG.

```
IGMP Debugging Information
--------------------------------------------------------------------------------
IGMP Debugging                  Enabled
Filter by group destination     224.1.2.3
Filter by source IP             10.10.1.123
--------------------------------------------------------------------------------
```

Table 2: Parameters displayed in the output of the SHOW IP IGMP DEBUG command.

Parameter	Meaning
IGMP Debugging	Whether or not IGMP debugging is enabled; one of "Enabled" or "Disabled".
Filter by group destination	The Group Destination Address specified by the DESTINATION parameter in the ENABLE IP IGMP DEBUG command. If the parameter was not given, "No" is displayed instead of the IP address.
Filter by source IP	The source IP address specified by the SOURCEIPADDRESS parameter in the ENABLE IP IGMP DEBUG command. If the parameter was not given, "No" is displayed instead of the IP address.

Examples To display IGMP debugging information, use the command:

```
SHOW IP IGMP DEBUG
```

See Also DISABLE IP IGMP DEBUG
ENABLE IP IGMP DEBUG

Checking the Port Map on Rapier16f*i* Switches

This section explains how to check that the port map on your Rapier16f*i* is correct. If the port map on your Rapier16f*i* is incorrect, this Note explains how to restore the correct settings.

This information is for Rapier16fi switches only.

The port map on your Rapier16f*i* will be incorrect if:

- it has software release 86s-251, but the 86251-04 patch is *not* loaded, or

- software release 86s-251 and patch 86251-04 are loaded, but the patch was corrupted after a restart or reboot.

The Rapier16f*i* requires the 86251-04 patch to operate correctly. Without this patch the port map is incorrect. An incorrect port map will cause problems if the configuration file refers to a port number.

The 2.5.3 software release for Rapier16fi switches will resolve this port map issue.

This section should be read in conjunction with the following document:

- Rapier Switch Documentation Set for Software Release 2.5.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

How to check that the port map is correct

The *ifIndex* and *Interface* fields in the SHOW INTERFACE command show the port map settings. *ifIndex* shows the index of the interface in the interface table, and *Interface* shows the physical or logical interface that maps to the index entry.

A correct port map

If the 86251-04 patch is successfully installed, and the port map is correct, the output from the SHOW INTERFACE command will be similar to that in Figure 1 on page 71.

Figure 1: Example output from the SHOW INTERFACE command *with* 86251-04.paz installed

```
Interfaces                                  sysUpTime:          00:00:09

DynamicLinkTraps.....Disabled
TrapLimit............20

Number of unencrypted PPP/FR links.....0

ifIndex Interface     ifAdminStatus   ifOperStatus     ifLastChange
--------------------------------------------------------------------------------
 1      port9         Up              Down                  00:00:00
 2      port10        Up              Down                  00:00:00
 3      port11        Up              Down                  00:00:00
 4      port12        Up              Down                  00:00:00
 5      port13        Up              Down                  00:00:00
 6      port14        Up              Down                  00:00:00
 7      port15        Up              Down                  00:00:00
 8      port16        Up              Down                  00:00:00
 9      port1         Up              Down                  00:00:00
 10     port2         Up              Down                  00:00:00
 11     port3         Up              Down                  00:00:00
 12     port4         Up              Down                  00:00:00
 13     port5         Up              Down                  00:00:00
 14     port6         Up              Down                  00:00:00
 15     port7         Up              Down                  00:00:00
 16     port8         Up              Down                  00:00:00
 17     vlan1         Up              Down                  00:00:00
--------------------------------------------------------------------------------
```

Although the *ifIndex* and *Interface* numbers do not match, *this is the correct port map*.

You do not need to take any more action if you have the correct port map.

An incorrect port map

If the 86251-04 patch is not installed, or has become corrupt, the output from the SHOW INTERFACE command will be similar to that in Figure 2 on page 72.

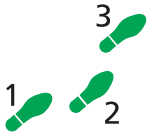
Figure 2: Example output from the SHOW INTERFACE command *without* 86251-04.paz installed

```
 Interfaces                                  sysUpTime:          00:01:22

DynamicLinkTraps.....Disabled
TrapLimit............20

Number of unencrypted PPP/FR links.....0

ifIndex Interface     ifAdminStatus   ifOperStatus     ifLastChange
--------------------------------------------------------------------------------
 1      port1         Up              Down                    00:00:00
 2      port2         Up              Down                    00:00:00
 3      port3         Up              Down                    00:00:00
 4      port4         Up              Down                    00:00:00
 5      port5         Up              Down                    00:00:00
 6      port6         Up              Down                    00:00:00
 7      port7         Up              Down                    00:00:00
 8      port8         Up              Down                    00:00:00
 9      port9         Up              Down                    00:00:00
 10     port10        Up              Down                    00:00:00
 11     port11        Up              Down                    00:00:00
 12     port12        Up              Down                    00:00:00
 13     port13        Up              Down                    00:00:00
 14     port14        Up              Down                    00:00:00
 15     port15        Up              Down                    00:00:00
 16     port16        Up              Down                    00:00:00
 17     vlan1         Up              Down                    00:00:00
--------------------------------------------------------------------------------
```

Although the *ifIndex* and *Interface* numbers match, *this port map is incorrect*.

You must restore the correct port map if your Rapier16f*i* shows this output.

How to restore the correct port map



The correct port map is restored with the following steps:

10. Force an EPROM download to restore the bootrom.

To force an EPROM download, you have to restart the switch. To restart the switch, use the command:

```
RESTART REBOOT
```

When the switch starts up, you will see the messages in Figure 3 on page 73.

Figure 3: Router startup messages

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 4096k bytes found.
INFO: BBR tests beginning.
PASS: BBR test, 128k bytes found.
PASS: BBR test. Battery OK.
INFO: Self tests complete
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download succeeded
INFO: Executing configuration script <boot.cfg>
INFO: Router startup complete
```

Enter [Y] when the `Force EPROM download (Y)?` option appears.

11. Load the 86251-04.paz patch file, and set it as the preferred patch.

To load the 86251-04.paz file, use the command:

```
LOAD FILE=86251-04.paz
```

To make this the preferred patch, use the command:

```
SET INSTALL=PREFERRED PATCH=86251-04.paz
```

12. Reboot the switch using the RESTART REBOOT command.

Once the switch has restarted, check that the patch has restored the correct port map settings using the SHOW INTERFACE command.

PPPoE Client on VLAN Interfaces

PPP over Ethernet (PPPoE) has two modes of operation: Client Mode and Access Concentrator (AC) mode. PPPoE can now be configured on Ethernet and VLAN interfaces in both modes.

To configure PPPoE in Client Mode, the physical-interface parameter VLAN*n-servicename* has been added, where *servicename* is 1 to 18 characters in length, and for a PPPoE client is usually supplied by the ISP providing the service. To specify that any service name is acceptable, you can use the special service name ANY.

The modified commands using the *VLANn-servicename* parameter are:

- ADD PPP
- CREATE PPP
- DELETE PPP
- SET PPP
- SHOW PPP

The modified commands and parameters are described below. For all other unmodified parameters and commands refer to the PPP Chapter in your software reference manual.

ADD PPP

Syntax

```
ADD PPP=ppp-interface OVER=physical-interface
   [other parameters]
```

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname*
  - VLAN*n-servicename*

Description

This command adds a lower layer interface or link to an existing PPP interface. This configures PPP multilink, which groups links together for increased bandwidth. The following may be added:

- a synchronous port
- a DS3 port
- an ISDN call
- an ACC call
- a MIOX circuit
- TDM group
- an L2TP call
- a PPP over Ethernet service over a VLAN interface

The OVER parameter specifies the physical interface over which the PPP interface will run. For PPP over Ethernet and PPP over VLAN links, use the service name provided by your ISP, or the special service name ANY to specify that any service is acceptable.

Examples

To add a PPPoE interface on VLAN2, using the service name ANY, as an additional physical interface to PPP interface 1, and enable STAC LZS compression on the synchronous link with a check mode of LCB, use the command:

```
ADD PPP=1 OVER=vlan2-any COMP=LINK STACCHECK=LCB
```

CREATE PPP

Syntax `CREATE PPP=`*`ppp-interface`* `OVER=`*`physical-interface`*
`[other parameters]`

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname* (L2TP tunnel)
  - VLAN*n-servicename*

Description This command creates the specified PPP interface running over:

- a synchronous port
- a DS3 port
- an ISDN call
- an ACC call
- a MIOX circuit
- TDM group
- an L2TP call
- a PPP over Ethernet service
- a PPP over Ethernet service over a VLAN interface

For PPP over Ethernet and PPP over VLAN links, use the service name provided by your ISP, or the special service name ANY to specify that any service is acceptable.

The OVER parameter specifies the physical interface over which the PPP interface will run. Additional physical interfaces can be added to the PPP interface using the ADD PPP command.

Examples To create PPP interface 0 `CREATE PPP=0 OVER=vlan2-access`

DELETE PPP

Syntax

```
DELETE PPP=ppp-interface OVER=physical-interface
   [other parameters]
```

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname*
  - VLAN*n-servicename*

Description This command deletes the specified lower layer interface from an existing PPP multilink bundle. The interface may be left with no lower layer interfaces.

The OVER parameter specifies the interface to be deleted.

Examples To delete the PPPoE service "*ANY*" on vlan2 as a physical interface from PPP interface 1, use the command:

```
DELETE PPP=1 OVER=vlan2-any
```

SET PPP

Syntax

```
SET PPP=ppp-interface [OVER=physical-interface]
   [other parameters]
```

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.
- *physical-interface* is:
  - SYN*n*
  - DS3*n*
  - ISDN-*callname*
  - ACC-*callname*
  - MIOX*n-circuitname*
  - TDM-*groupname*
  - TNL-*callname*
  - VLAN*n-servicename*

Description This command is used to change the configuration parameters of a PPP interface running over:

- a synchronous port
- a DS3 port
- an ISDN call
- an ACC call
- a MIOX circuit
- TDM group
- an L2TP call PPP over Ethernet service
- a PPP over Ethernet service over a VLAN interface

For PPP over Ethernet and PPP over VLAN links, use the service name provided by your ISP, or the special service name ANY to specify that any service is acceptable.

SHOW PPP

Syntax `SHOW PPP[=`*`ppp-interface`*`]`

where:

- *ppp-interface* is the PPP interface number, from 0 to 511.

Description This command displays a list of each PPP interface, users of the interface, physical interfaces that the interface is running over, and the current state of the interface.

There have not been any changes to the descriptive text or SHOW output in this command. The only change is in the Table. Table 1 shows the row which has changed, with the changed text in **bold**.

Table 3: Parameters displayed in the output of the SHOW PPP command (showing the changed row only).

Parameter	Meaning
Over	The lower layer(s) used by the PPP interface; SYN*n*, DS3*n*, ISDN-*callname*, ACC-*callname*, MIOX*n-circuitname*, TDM-*groupname*, **VLAN*n-servicename*,** TNL-*callname*.